August, 1995

Dear Colleague:

Enclosed is INPUT's report entitled *Federal Computer Security Market 1995*, issued as part of INPUT's Federal Information Technology Program.

The report's findings are based on analyses of agency programs, OMB and agency *Five-Year Information Technology Plans for 1995–2000*, and agency and vendor interviews. The report focuses on security products and services and is designed to help vendors plan their strategies to compete for federal security contracts.

This federal market report was designed by INPUT as an update to the 1992 report concerning the market for security in federal information processing systems. This report was prepared in response to client interest in this market and identifies market issues and trends.

If you have any questions or comments regarding this report, please do not hesitate to contact us.

Sincerely,

Robert W. Deller
Vice President

Enc.

Federal Computer Security Market 1995

INPUT®

INPUT

STRATEGIC MARKET PERSPECTIVE

Federal Computer Security Market 1995

Federal IT Market Analysis Program

1995

Federal Computer Security Market

1995

INPUT

Frankfurt • London • New York • Paris • San Francisco • Tokyo • Washington, D.C.

Abstract

INPUT expects the federal government market demand for computer security products and services to grow from $584 million in FY 1995 to $790 million in FY 2000. This represents a compound annual growth rate (CAGR) of 6%. This estimate excludes classified processing, because these data cannot be captured.

Federal Computer Security Market 1995 covers the forces, both positive and negative, driving this market. This report revisits research conducted in 1992 pertaining to this market and cites several significant changes. It also identifies which agencies will buy, how much will be bought, how it will be bought, and who will do the buying. The report compares agency and vendor perceptions of the market, and suggests some steps for vendors to take in expanding their market share.

This report contains 117 pages including 42 exhibits.

© 1995 by INPUT. Reproduction Prohibited.

Research by
INPUT
1921 Gallows Road
Suite 250
Vienna, VA 22182
United States of America

Published by
INPUT
1881 Landings Drive
Mountain View, CA 94043-0848
United States of America

Federal Information Technology Market Analysis Program

Federal Computer Security Market

Copyright © 1995 by INPUT. All rights reserved. Printed in the United States of America. No part of the publication may be reproduced or distributed in any form, or by any means, or stored in a database or retrieval system, without the prior written permission of the publisher.

The information provided in this report shall be used only by the employees of and within the current corporate structure of INPUT's clients, and will not be disclosed to any other organisation or person including parent, subsidiary, or affiliated organisation without prior written consent of INPUT.

INPUT exercises its best efforts in preparation of the information provided in this report and believes the information contained herein to be accurate. However, INPUT shall have no liability for any loss or expense that may result from incompleteness or inaccuracy of the information provided.

MMA6 • 740 • 1995

Table of Contents

I	Introduction	I-1
	A. Scope	I-2
	B. Methodology	I-2
	C. Report Organization	I-4
II	Executive Overview	II-1
	A. Federal Market Pressures	II-1
	B. Market Forecast	II-4
	C. Government Planning and Review	II-5
	D. Performance Criteria	II-6
	E. Acquisition Methods	II-6
	F. Recommendations	II-7
III	Market Analysis and Forecast	III-1
	A. Market Evaluation and Development	III-1
	B. Market Structure	III-8
	C. Market Forecast	III-11
	1. Civilian Market	III-11
	2. Defense Market	III-12
	D. Federal Market Pressures	III-16
	E. Laws, Regulations and Policies	III-18
	F. Key Federal Agencies	III-19
	1. General Services Administration	III-19
	2. Office of Management and Budget	III-20
	3. National Security Agency	III-20
	4. National Institute of Standards and Technology	III-21
IV	Federal User Requirements and Trends	IV-1
	A. Security Plans: Implementation and Compliance	IV-1
	1. Purpose of Security Plan	IV-2
	2. Effectiveness of Security Plan	IV-3

© 1995 by INPUT. Reproduction Prohibited.

3. Security Plan Coverage IV-3
4. Review of Security Controls IV-5
5. Written Authorization for System Use IV-5

B. Directives and Guidelines IV-5
1. Directives and Guidelines Used IV-6
2. Impact of Appendix III to OMB Circular A-130 IV-7

C. Future Computer Security Measures IV-7
1. Acquisition of Administrative Services IV-8
2. Acquisition of Hardware IV-9
3. Acquisition of Physical Security IV-9
4. Acquisition of Software IV-10
5. Acquisition of Other Security IV-11

D. Implementation and Access IV-11

E. Functional Requirements and Performance Criteria IV-12
1. Performance Criteria Priority IV-12
2. Success of Products in Meeting Current Criteria IV-13
3. Selection Criteria for Security Products and Services IV-14

F. Acquisition Plans and Preferences IV-15
1. Acquisition Methods IV-15
2. Most Appropriate Vendor IV-16
3. Use of GSA Contractors IV-17

G. Vendor Performance IV-18

H. Impacts and Trends IV-19
1. Security Policy Impact on Electronic Commerce IV-19
2. Effects of Technology on Security Requirements IV-20
3. Impact of Non-Technical Market Factors IV-21
4. Impact of Budget Levels IV-21
5. Impact of Government Policies and Regulations IV-23

V Competitive Trends V-1

A. Vendor Participation V-1
1. Vendor Products and Services V-1

B. Vendor Market Perceptions V-2
1. State of the Federal Computer Security Market V-2
2. Growth Factors in the Federal Computer Security Market V-3
3. Leading Opportunities V-4
4. Market Differences V-5
5. Competitive Advantages of the Fed. Computer Security Market V-6

C. Vendor Performance V-7
1. Ratings of Vendor Performance V-7
2. Suggested Improvements to Products and Services V-8

D. Teaming Patterns V-9

© 1995 by INPUT. Reproduction Prohibited.

1. Success of Teaming Efforts V-9
2. Preferred Teaming Partners V-9
E. Trends V-11
1. Technology Trends V-11
2. Budgetary Constraints V-11
3. Market Trends V-12

A Federal Agency Respondent Profile A-1
A. Vendor Respondent Profile A-2

B Glossary of Federal Acronyms B-1
A. Federal Acronyms B-1
B. General and Industry Acronyms B-2

C Policies, Regulations and Standards C-1
A. OMB Circulars and Bulletins C-1
B. DoD Directives C-1
C. Standards C-1

D OMB Circular A-130 Appendix III D-1

E Related INPUT Reports E-1
A. Annual Market Sales E-1
B. Market Reports E-1

F Questionnaires F-1
A. Agency Questionnaire F-1
B. Vendor Questionnaire F-8

G Computer Security Opportunities G-1

H Security Vendors H-1
A. Security Devices H-1
B. FAX Security H-1
C. Secure LANS H-2
D. Secure Modems H-2
E. Security Software H-3

© 1995 by INPUT. Reproduction Prohibited.

F. Security Systems Software H-4
G. Security Consulting H-5

© 1995 by INPUT. Reproduction Prohibited.

Exhibits

II	-1	Federal Market Pressures	II-1
	-2	Computer Security Market, FY 1995–2000	II-4
	-3	Performance Criteria Priority	II-6
	-4	Acquisition Methods	II-7
III	-1	Computer Security Issues	III-6
	-2	Computer Security Levels	III-7
	-3	Federal Computer Security Market, 1995–2000	III-11
	-4	Civilian Computer Security Market, 1995–2000	III-12
	-5	Defense Computer Security Market, 1995–2000	III-13
	-6	Key Management Controls	III-14
	-7	Federal Computer Security Market Pressures	III-17
	-8	Computer System Security and Privacy Advisory Board	III-22
IV	-1	Purpose of Security Plan	IV-2
	-2	Effectiveness of Security Plan	IV-3
	-3	Security Plan Coverage	IV-4
	-4	Directives and Guidelines Used	IV-6
	-5	Impact of Appendix III to OMB Circular A-130	IV-7
	-6	Acquisition of Administrative Services	IV-8
	-7	Acquisition of Hardware	IV-9
	-8	Acquisition of Physical Security	IV-10
	-9	Acquisition of Software	IV-10
	-10	Acquisition of Other Security	IV-11
	-11	Performance Criteria Priority	IV-13
	-12	Success of Products in Meeting Current Criteria	IV-14
	-13	Selection Criteria for Security Products and Services	IV-15
	-14	Acquisition Methods	IV-16
	-15	Most Appropriate Vendor	IV-17
	-16	Vendor Performance Ratings	IV-18
	-17	Security Policy Impact on Electronic Commerce	IV-19
	-18	Factors of Technological Change	IV-20
	-19	Impact of Non-Technical Market Factors	IV-21

© 1995 by INPUT. Reproduction Prohibited.

-20 Impact of Budgetary Levels IV-22
-21 Impact of Government Policies and Regulations IV-23

V

-1 Types of Security Products and Services Provided V-2
-2 State of the Federal Computer Security Market V-3
-3 Growth Factors in the Security Market V-4
-4 Federal Agency Opportunities V-5
-5 Competitive Advantages of the Federal Market V-6
-6 Comparative Ratings of Vendor Performance V-7
-7 Suggested Improvements for Security Products and Services V-8
-8 Success of Teaming Efforts V-9
-9 Most Preferred Teaming Partner V-10

© 1995 by INPUT. Reproduction Prohibited.

Introduction

The *Federal Security Market 1995* is an update of INPUT's 1992 report concerning the market for security of federal information processing systems. The report was prepared in response to client interest in this market and identifies market issues and trends that impact current federal contractors and vendors entering into, or already in, the information security market through FY 2000. Insight into agency requirements, regulations and contractor perceptions are offered to help vendors plan their strategies to compete for federal security contracts.

This report on security products and services applicable to the federal government was prepared as part of INPUT's Federal Information Technology Market Program (FITMP). Reports issued through this program are designed to assist INPUT's U.S. industrial clients in planning how to satisfy future federal government needs for computer-based information systems and services. The report's findings are based on research and analyses of several sources, including:

- INPUT's Procurement Analysis Reports (PARs)
- OMB/GSA/NBS Five-Year Information Technology Plans for 1995-2000
- Interviews with agency representatives
- Interviews with leading vendors pursuing the federal computer security market
- Interviews with representatives from the Computer Systems Lab of the National Institute of Standard and Technology (NIST)
- Federal Agency FY 1994 and FY 1995 Information Technology Plans
- Federal reports, studies, and other secondary research sources.

© 1995 by INPUT. Reproduction Prohibited.

The current proposal by the Office of Management and Budget (OMB) to revise Appendix III of Circular No. A-130, "Security of Federal Automated Information Systems" is intended to guide federal agencies in securing information as they increase utilization of an open, interconnected National Information Infrastructure. This initiative, the third stage of revisions to Circular A-130, is a continuation of the security improvement process mandated by the Computer Security Act of 1987 and furthered by OMB Bulletins 88-16 and 90-08. In incorporating and updating the policies set out in those bulletins, this revision provides a foundation for defining a changing federal market for security applications.

A
Scope

The forecast period covered in the report is FY 1995 through 2000. Agency and vendor surveys were conducted for this report update.

For the purpose of this 1995 study, INPUT's definition of computer security incorporates the following categories of vendor products and services:

- Hardware
- Software products
- Professional services

This report supplements INPUT's preceding reports on professional services. It is intended to give INPUT clients a clearer understanding of the current status and future trends in the federal market for computer security. It also identifies the key vendors in the market, a subject of continuing interest to INPUT clients.

B
Methodology

In developing this report, INPUT utilized a variety of sources and methods. Agency long-range plans were researched and budget submissions for FY 1995–2000 for major programs were reviewed. INPUT examined new initiatives involving security of information processing systems and, based on this research, pinpointed agencies and programs that relate to computer security.

Central to this undertaking is an inclusive definition of computer security:

© 1995 by INPUT. Reproduction Prohibited.

ANSI Standard X3.172A (1992)

Computer Security. 1. Configuration, technology, technical measures, and administrative measures used to protect hardware, software and data of an information processing system from deliberate or inadvertent unauthorized acquisition, damage, destruction, disclosure, manipulation, modification, use or loss. 2. Protection resulting from the application of computer security.

OMB Circular No. A-130, Appendix III (March 22, 1995, Proposed)

Adequate Security. Security commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information.

Traditional

Information Security. The preservation of the confidentiality, integrity, and availability of information, the "CIA of security."

Focusing on the definition contained in OMB's (proposed revision of) Circular No. A-130 Appendix III, INPUT based its research on a market definition evolving from expanding agency reliance on an increasingly open and interconnected National Information Infrastructure. The recommendations of the National Performance Review, "Creating a Government that Works Better & Costs Less: Reingineering through Information Technology" (September, 1993) and the Computer System Security and Privacy Advisory Board, established by the Computer Security Act, support the proposed revision of Circular A-130 Appendix III to recognize the changing nature of security management. INPUT's research and analysis address this impact on federal programs and recognize strategic requirements in this evolving market.

INPUT reviewed its Procurement Analysis Reports (PARs—part of the Federal Information Technology Procurement Program) to develop further insight on agency activities. Many PARs cover programs that, for one reason or another, do not appear in the agency budget submissions. The PARs yield additional possibilities for further research. INPUT also interviewed federal agency executives at the policy level to identify current trends and issues relevant to the federal computer security market. INPUT developed a special questionnaire for the agency interviews (Appendix F).

The current versions of the Federal Information Resource Management Regulations, Federal Acquisition Regulations, Defense

© 1995 by INPUT. Reproduction Prohibited.

Acquisition Regulations, and relevant federal legislation and agency regulations were investigated to identify provisions that will impact computer security contracts and contract performance.

C
Report Organization

In addition to the introduction and appendices, this report consists of five chapters:

- Chapter II contains an executive overview describing the major points and findings in the report.
- Chapter III provides the market forecast and describes the major market issues and trends impacting the industry.
- Chapter IV summarizes the federal agencies' requirements for computer security and the existing and planned implementation of security requirements.
- Chapter V presents vendors' perspectives on the federal computer security market.

Several appendices are also provided:

- Interview profiles
- Glossary of Federal Acronyms
- Policies, Regulations and Standards
- OMB Circular A-130 Appendix III
- Related INPUT Reports
- INPUT Questionnaire
- Computer Security Opportunities
- Security Vendors

© 1995 by INPUT. Reproduction Prohibited.

II

Executive Overview

A
Federal Market Pressures

The federal market for computer security products and services is expected to grow over the next five years. Exhibit II-1 lists, in both positive and negative terms, some of the forces affecting this growth.

Exhibit II-1

Federal Market Pressures

- Policy initiatives
- National Performance Review
- Electronic delivery of services
- Increased Internet use
- Publicized security breaches
- Budget constraints

Source: INPUT

The Computer Security Act of 1987 is at the apex of the pyramid of laws, regulations and policy directives aimed at safeguarding information in federal agencies. It requires the development of computer security plans and the initiation of computer security training in each federal agency. OMB issued Bulletin No. 88-16, "Guidance for Preparation and Submission of Security Plans for Federal Computer Systems Containing Sensitive Information," July 6, 1988, and Bulletin No. 90-08, "Guidance for Preparation of Security Plans for Federal Computer Systems Containing Sensitive Information," July 9, 1990, to assist agencies in implementing the Act.

A pending revision of Appendix III of OMB Circular No. A-130, "Security of Federal Automated Information," due by the beginning of FY 1996, is central to the improvement of federal information security practices. This

© 1995 by INPUT. Reproduction Prohibited.

revision takes into account the intent and provisions of the Computer Security Act and the observations regarding security plans and practices made during a series of agency visits in 1992.

OMB, in conjunction with NIST and the National Security Agency (NSA), made the agency visits and subsequently produced "Observations of Agency Computer Security Practices and Implementation of OMB Bulletin No. 90-08." Their review found both insufficient incentives for compliance and insufficient sanctions for noncompliance with the intent of the Computer Security Act. Agencies have developed required security plans; nevertheless, a requirement for periodic review and update is lacking. Even as technologies and operations evolve, security systems and oversight tend to atrophy over time in the absence of any reminder of their importance.

The revision of Appendix III of Circular No. A-130, according to OMB, "is intended to guide agencies in securing information as they increasingly rely on an open and interconnected National Information Infrastructure (NII). It stresses management controls such as individual responsibility, awareness and training, and accountability, rather than technical controls. For example, it would require agencies to assure that risk-based rules of behavior are established, that employees are trained in them, and that the rules are enforced. The proposal would also better integrate the need for centralized reporting of paper security plans, emphasize the management of risk rather than its measurement and revise government-wide security responsibilities to be consistent with the Computer Security Act."

As agencies shift computing power to the desktop, enhance information sharing through local- and wide-area networks, and move to electronic delivery of services to the citizen, security risks increase with the ease of sharing information over more open networks. The National Performance Review (NPR) emphasizes the need for information security through the development of standard encryption capabilities and digital signatures to protect sensitive but unclassified data and systems, as well as a comprehensive Internet security plan, and it recommends the revision of OMB Circular A-130 to require enhanced security measures. The NPR also directs NIST to coordinate a government-wide plan for research and development addressing a wide range of security issues, and supports the security concerns of the NII initiative. NIST's Security Criteria and Evaluation project and Secure the Internet and Network Connectivity project address Internet and NII security issues with plentiful commercial security solutions as their objective.

Increased awareness of security breaches is felt by many federal agency executives. Information security and privacy problems have received much media coverage, since the well-publicized Internet virus attack of

© 1995 by INPUT. Reproduction Prohibited.

November, 1988. From April, 1990 to May, 1991, 34 Department of Defense (DoD) locations experienced penetration of computer systems by hackers through Internet access. IRS auditors, in November, 1992, identified widespread employee misuse of taxpayer account data, and in July, 1993, misuse of the FBI's National Crime Information Center data by authorized users was publicized. Since the February, 1994, warning by the Computer Emergency Response Team of such activity, hacker attacks have increased significantly on military and government computer systems with password-capturing sniffer programs. As a result, information security is achieving new prominence.

Budget constraints, however, act to discourage the growth of federal computer security. Continuing pressure to reduce expenditures is the biggest single inhibitor. Oversight agencies face not only cuts but threatened elimination, and operating agencies must deal with choices between enhanced security and operational effectiveness. Many agencies are forced to allocate limited resources to more pressing initiatives than information security, whenever the payoff seems greater.

Many senior agency executives and congressional overseers do not appreciate the potential losses from security incidents, until after they have occurred. Significant market changes do not appear until after major disasters have taken place, possibly involving major property loss and even the loss of life. Consequently, despite several attempts, Congress has failed to pass any follow-up legislation to the Computer Security Act. Diminishing congressional concern has compounded a lessening in appropriations supporting information security. More attention has been drawn to the administration's escrowed encryption standard (Clipper) and a proposed congressional review, by the National Research Council, of cryptography policy.

Estimates of financial losses, while essential to the process of managing risk, have had little prominence in the development of agency security plans. Although development of plans, spurred by the Computer Security Act, can be considered a positive factor, the quality of plans produced may be viewed as a negative. Security managers, while attempting to use a top-down and ongoing process, often are limited by budgetary constraints to ad hoc approaches for the protection of information. The application of security products and services sometimes lacks an overall formal process. Consequently many plans:

- Ignored user organization involvement
- Failed to gain ownership by top management
- Overlooked critical human factors in information security.

© 1995 by INPUT. Reproduction Prohibited.

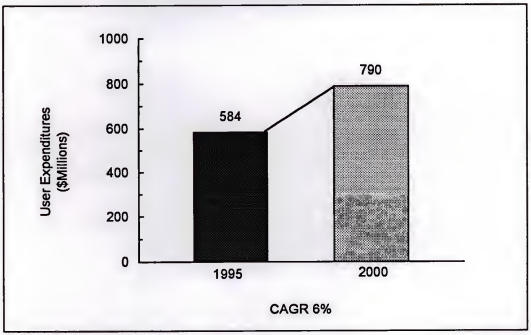
The implication, for many agencies, is that planning required by the Computer Security Act is little more than a paperwork exercise.

B
Market Forecast

INPUT expects that the federal computer security market will grow from $584 million in FY 1995 to $790 million in FY 2000, at a compound annual growth rate (CAGR) of 6%. Exhibit II-2 displays the overall forecast.

Exhibit II-2

Computer Security Market, FY 1995–2000



Source: INPUT

Hardware products will show the fastest growth rate, as agencies use them both to improve existing systems and to evolve new solutions to the challenges of open architectures and information sharing. Integrated solutions, contained under hardware in the INPUT forecast model, will show a similarly healthy rate of growth as encryption-based products gain market share. The software market will remain fairly modest at a CAGR of only 3%, evidencing:

- A preponderance of small purchases off IT budgets
- Growth of commercial off-the-shelf products
- Developing availability of hardware-based solutions.

© 1995 by INPUT. Reproduction Prohibited.

The market for professional services will maintain the same pace as software, continuing a slow but steady pattern of growth.

Network security consists of products such as secure operating system software and hardware-based encryption. It is excluded from INPUT's forecast model because of the embedded nature of its processing. However, it represents a significant business opportunity in the federal market. Because of increasing use of LANs and WANs and accelerating Internet utilization, this market will continue to grow at a healthy rate.

C
Government Planning and Review

In May 1990, the General Accounting Office (GAO) issued a report, "Computer Security: Governmentwide Planning Process Had Limited Impact" (GAO/IMTEC-90-48), that stated that the planning and review process implemented under the Computer Security Act did little to strengthen computer security governmentwide. While agency officials believed that awareness of computer security issues was heightened by the process, they typically found the plans of limited use in addressing agency-specific problems and viewed them as merely reporting requirements.

Officials, whose agency plans and processes were reviewed by GAO, cited three problems relating to the design and implementation of the planning process:

- The plans lacked adequate information to serve as management tools
- Managers had little time to prepare the plans
- OMB planning guidance was sometimes unclear and was misinterpreted by agencies.

GAO's review, the fifth in a series of reports on the implementation of the implementation of the Computer Security Act prepared for the House Committee on Science, Space and Technology, was made the year after initial computer security plans were completed. The report concluded that "agencies have made little progress in implementing planned controls. Agency officials said that budget constraints and inadequate top management support -- in terms of resources and commitment -- were key reasons why controls had not been implemented."

© 1995 by INPUT. Reproduction Prohibited.

D
Performance Criteria

A survey was conducted by INPUT in order to collect data for this report. Results of the survey of performance criteria are shown in Exhibit II-3. Most agency respondents provided more than one answer and all agreed on the need for continued service. This response suggests the importance that agencies assign to the continued operation of information processing services and mission-critical applications.

Exhibit II-3

Performance Criteria Priority

Criteria	High	Low	None
Continued Service	20	4	0
Access Control	19	3	1
Back-up and Recovery Provisions	19	3	1
No Security Breaches	14	7	2
Physical Security	14	8	0
Other	0	0	0

Total responses = 24 *Source: INPUT*

Access control and back-up and recovery provisions were tied for a close second, highlighting the risks and threats of greatest concern to federal agencies. In INPUT's view, these accurately reflect agency needs in computer security. Functional safeguards to assure limited and proper access to sensitive data include encryption techniques, passwords, and multilevel secure (MLS) operating systems. Physical security, often the least costly requirement, includes access to data centers, remote processing sites, and any additional LAN or WAN sites.

E
Acquisition Methods

The ranking of methods used most often for acquisition was actually too close to call. There was not one method that was used significantly more often than any other. Exhibit II-4 shows the results of this survey question, which queried most often used methods, as well as all methods utilized.

© 1995 by INPUT. Reproduction Prohibited.

Exhibit II-4

Acquisition Methods

	Number of Responses	Percent of Respondents
GSA Schedules	14	58
RFPs for Specific Purchase	14	58
RFP for Requirement Contract	13	54
Purchase as Part of Other Procurements	13	54
Other	4	17
Most often used:		
RFP for Requirement Contract	6	
GSA Schedules	1	

Total Responses = 24 *Source: INPUT*

RFP for requirements contract and purchase as part of other procurements received equal ratings from agency respondents, placing a close second and supporting a growing trend toward use of requirements contracts noted in INPUT's 1992 security report.

Additionally, INPUT's survey queried agencies for most often used method of acquisition, with the result that one-fourth of the respondents cited RFP for requirements contract and only one noted GSA schedules.

Security products and hardware increasingly are being acquired as part of other procurements, such as the Treasury Department's Treasury Communications System (TCS), the USAF's Defense Message System (DMS), and in Multilevel Information Systems Security Initiative (MISSI)-influenced DoD procurements. Additionally, most systems integration solicitations contain security requirements as integral with other functional requirements.

F
Recommendations

Vendors must opt for a flexible approach in providing security products and services to the federal government. Their efforts must address the increased risk and vulnerability resulting from the networking of federal information systems. Agency issues requiring vendor attention are:

- Cost-justifying safeguards
- Internet security

© 1995 by INPUT. Reproduction Prohibited.

- Electronic commerce
- Encryption
- Emergence of COTS solutions.

With continuing congressional pressure on agencies, spending is not likely to increase more than forecast. Vendors need to incorporate security solutions as part of other offerings, such as network implementation and management, and professional services.

Many agency purchases of security improvements will come through systems integration contracts that are not focused specifically on computer security. Consequently, vendors specializing in computer security should develop teaming relationships that enable participation in large, complex procurements.

The wide range of systems and varied types of equipment and software utilized by the federal government present a development challenge to security vendors. To the extent that security solutions accommodate widely varying systems and emerging federal standards, the potential for increased market penetration is good.

Continuing agency deficiencies in training and awareness, planning and implementation, and effective security management manifest a significant opportunity for vendors. Many agencies still fall short in these areas and need support in monitoring, managing, and upgrading their computer security. Additional help is needed in developing contingency plans. Vendors positioned to help with these management issues will gain a competitive advantage.

Recommendations

- Address increased risk from networking
- Forge effective teaming relationships
- Develop interoperable standards-based products
- Provide essential training tools
- Support fundamental awareness and management issues.

© 1995 by INPUT. Reproduction Prohibited.

III

Market Analysis and Forecast

A
Market Evaluation and Development

Computer security for the federal government focuses on protecting the confidentiality, integrity and availability of information assets contained in federal automated systems. It also includes assuring the accuracy and accessibility of information so that the public can be informed and agencies can discharge their duties efficiently and responsively. In support of federal agency missions, computer security assists with the management of systems in performing appropriate functions. Security works to protect information in these systems from threats such as unauthorized disclosure and unauthorized or inadvertent modification and ensures that information is available on a timely basis.

Threats are events or agents that have the potential to cause harm to a system or to its information assets. These threats have the potential to exploit the network's many vulnerabilities. New vulnerabilities emerge as systems are built or changed or networked. Multiple threats often combine to expose vulnerabilities to networked information, such threats are grouped in the following categories:

- Human errors and design faults
- Insiders
- Natural disasters and environmental damage
- Hackers, viruses and other malicious software.

It is instructive to note that three of the above-cited categories deal with human rather than technical factors. This shift in emphasis, from a traditional focus on technical factors enabling confidentiality and access control, warrants attention from both federal security managers and vendors. Federal agencies utilize security safeguards to provide

© 1995 by INPUT. Reproduction Prohibited.

protection against disclosure, modification or destruction of networked information. These safeguards include hardware, software, physical controls, user procedures, administrative procedures and management and personnel controls.

Information networks are described as any set of interconnected electronic information systems, computers, magnetic drives, optical systems, telecommunications systems and other data control and transmission units. Consequently, a network is not restricted to the Internet, inter-agency networks, any other intra-agency proprietary network, or the public switched telephone network (PSTN). In today's environment, distinctions are difficult to make as networks become increasingly interconnected and meshed.

Security functions to protect information in automated systems from unauthorized disclosure and unauthorized or inadvertent modification, and also ensures that information is available on a timely basis. In many federal systems, however, it is important to point out that protection from disclosure is not the primary security issue because information is intended for widespread dissemination to the public. Safeguards for automated information systems, to be successful, must be organized and applied in a coordinated fashion to contain risks from the above-cited threats while at the same time maintaining network and system functionality. Reasonable safeguards may include:

- Expressing organizational objectives
- Writing an organizational security policy
- Cost-justifying safeguards
- Developing formal security models
- Incorporating specific safeguard techniques and tools.

The single most important step toward implementing proper safeguards for networked information in a federal agency is for top management to define the agency's overall objectives, define a security policy to reflect those objectives, and implement that policy. Only top management can consolidate the consensus and apply the resources necessary to protect networked information. Without understanding and support from top management, an organization's deployment of safeguards can be completely ineffective. Effectiveness requires guidance from OMB, commitment from top agency management, and oversight from Congress. The security policy of an agency is intended to implement the overall objectives, express the organization's philosophy on management of risk

© 1995 by INPUT. Reproduction Prohibited.

and assign responsibilities. A written policy is essential to define requisite safeguards.

Various federal agencies have conflicting missions and policies. Growing pressure to make government more efficient often complicates the need to protect copyrighted, private and proprietary information. Agencies historically have delivered their services in a "stovepipe" fashion, managing information services vertically within the agency but not horizontally across agency boundaries. Networked information systems make horizontal exchanges of information much easier, but such sharing also brings new risks because different agencies and non-government users have different objectives and policies regarding information security. A great need exists for agencies and other organizations to develop sound security policies that match the reality of modern information networks and to anticipate a future in which more information will be shared among agencies and organizations.

Information never can be secured absolutely. Therefore, safeguarding information is not a matter of how to secure the information, but how much security an agency can justify. Approaches range from effective and inexpensive to very costly for both small and large organizations. Therefore, risk analyses must be applied to balance the cost of the safeguard with the potential loss that can occur if the safeguard is not utilized. Alternatively, agencies can use a due-care or reasonable-care approach to determine how much security is affordable. Such an approach seeks an acceptable level of safeguards relative to other agencies and businesses, as opposed to an acceptable level relative to an absolute measure of risk. Given a set of objectives and a stated policy, a formal model can be developed to express a more specific policy in a way that can be tested. A specification process is derived from the model and provides a method to ensure implementation. Thus, the formal process provides a series of steps for isolation and testing. An example of a well-known security model is the Bell-La Padula Model, applied to the protection of the confidentiality of classified information in multi-level security classifications.

The commercial marketplace provides security products and services that range from simple devices such as a metal key used to secure a personal computer at night to elaborate encryption techniques and digital signatures. Tools and techniques alone do not safeguard information. Expert personnel are required to apply and maintain them, and they must be combined in a coordinated fashion to meet agency objectives such as confidentiality, integrity, availability or any other attributes of security.

© 1995 by INPUT. Reproduction Prohibited.

Classes of techniques and tools currently available include:

- Challenge-response systems
- Secure tokens
- Firewalls
- Virus checkers
- Auditing and intrusion detection
- Encryption
- E-mail and digital signatures
- Biometric devices
- Separation of duties.

Attacks on password systems can be deterred by challenge-response systems that never actually send a password over a network. When a user logs on, the central computer issues a random challenge. The user transcribes the challenge and the password into an authenticator, which calculates a unique response. The user then sends that response to the central computer, which repeats the calculation and then compares its result with the user's result. An intruder cannot imitate the user without access to an identical authenticator and its associated password. Secure tokens also can substitute for the authenticator. A user's token can generate a response based on a unique secret key and the local time, instead of a challenge from the central computer.

Secure tokens, smart cards, Personal Computer Memory Card International Association (PCMCIA) cards and smart disks are secure token devices used to authenticate users to computers. In an access control system, the token must be inserted into a reader connected to a computer which may be connected to a network. Then the token obtains access on behalf of the user by providing necessary authorization and confirming the user's identity.

A firewall provides a focus for managing network safeguards by restricting communication into and out of the network. The firewall itself is in a dedicated computer that examines and restricts mainly incoming, but sometimes outgoing, communications.

Virus checkers are software programs that automatically search computer files for known viruses and scan files every time the computer is turned on or when new memory media are inserted into the computer. As new

© 1995 by INPUT. Reproduction Prohibited.

viruses are discovered every month, it is imperative that virus checkers be updated often.

Auditing is the automatic monitoring of certain transactions occurring in a network over a period of time, including file transfers and the local time when users access the network. Large volumes of information about network use often are generated, relegating auditing to an activity in which records are kept only for later examination. This method is only a passive deterrent to authorized users who might fear getting caught if an investigation takes place. Integrated, dynamic auditing systems not only record information but also restrict use or alert security personnel when possible violations occur, not just by outsiders but by insiders as well. Some sophisticated systems use expert systems that learn users' behavior, to monitor systems for unusual activity.

Encryption is used in a variety of applications, including the protection of confidentiality and integrity, and authentication and non-repudiation. Different methods include symmetric and asymmetric cryptosystems. The former is also called a single key or secret key system, as utilized by the Data Encryption Standard (DES). Asymmetric, or public key, systems use one key to encrypt and a second different, but mathematically related, key to decrypt.

Access control systems utilize three methods to identify particular users: something the user knows, as a password; something in the user's possession, as a secure token; and something that physically characterizes the user, known as biometrics. Characteristics that might be analyzed include retinal scans, fingerprints, hand prints, voice prints, signature dynamics and keystroke patterns.

Safeguards can be based on administrative procedures as well as on hardware or software solutions. Authority and capacity to perform certain functions with networked information can be separated and delegated to varying individuals. A procedure can be applied to separate the authority to add users to a system and other administrative duties from the authority to assign passwords, review audits and perform security administration. Wiretap laws apply the separation of duties principle by requiring law enforcement personnel to obtain permission from courts before proceeding. The current administration's key escrow encryption initiative applies the separation of duties principle in storing key components with two escrow agents, however, in the original proposal both are in the executive branch.

Many individual safeguard tools and techniques currently are available to adequately address automated information vulnerabilities, provided users know what to purchase and can afford to use the solution correctly. More affordable, easier to use safeguards are needed, particularly general

© 1995 by INPUT. Reproduction Prohibited.

purpose products that integrate multiple security features with other functions.

Federal government regulation and management of security of its automated information systems has an extensive history of legislative and regulatory initiatives and executive policies. These are discussed in section E of this chapter.

Exhibit III-1 summarizes some key security issues.

Exhibit III-1

Computer Security Issues

- Near-Term Compliance
- Oversight Coordination
- Growth Expectations
- New Emphasis in Security Management
- Scarce Resources

Source: INPUT

A continuing problem for agencies arises from the retrofitting of existing systems with required security features. Computer security is being specified in the development of new systems, but bringing current automated information systems up to new standards is more difficult. The shift to management of risk, rather than its measurement under Appendix III of OMB Circular A-130, should reduce the need for paper security plans and centralized reporting. The adoption of integrated security features addresses the reality of limited resources faced by federal managers.

Oversight coordination is a continuing need, both among and within agencies governing security policy. Contingency plans and disaster recovery plans still do not exist at some agencies, and many agencies that have plans have not implemented or tested them. There is, as well, a continuing need for better coordination among the General Services Administration (GSA), OMB and NIST for monitoring security compliance and standards development. OMB's Circular A-130 is the basic IT management policy document for the federal government, and the pending Appendix III focuses on user behavior and risk management. In addressing the security problems associated with increasing public access, OMB reaffirmed the role of NIST in developing federal security standards and guidance for civilian agencies.

INPUT expects to see more growth than previously reported in this market. As more open systems evolve and technology advances, vulnerability rises. Increased networking among automated information

© 1995 by INPUT. Reproduction Prohibited.

systems demands new and adaptive approaches to security management. Concurrently, interest is rising in compliance issues associated with the new security portion of OMB Circular A-130. Stressing management of risk and individual responsibility, the pending Appendix III emphasizes securing information and focuses on human factors. Behavior and access rules should become central to the management of computer security, with less emphasis than before on securing equipment. Continuing awareness and training programs, and triennial reviews and audits of security controls will be required of federal agencies under the new security appendix.

Information security places additional demands on already scarce agency resources. Faced with the expense of retrofitting systems, some agencies are adopting a systems life cycle approach to security. While a continuing need for funding to support the implementation of security plans, training and controls exists across agencies, the evolving nature of technology, standards and requirements should enable more cost-effective solutions.

Information security concerns at the Department of Defense lead to the publication, in 1983, of DoD Trusted Computer System Evaluation Criteria (TCSEC), often called the Orange Book, which establishes a hierarchy of computer security ranking, shown in Exhibit III-2.

Exhibit III-2

Computer Security Levels

- Division A: verified protection
  - Class A1: verified design
  - Beyond Class A1: future technology
- Division B: mandatory protection
  - Class B1: labeled security protection
  - Class B2: structured protection
  - Class B3: security domains
- Division C: discretionary security protection
  - Class C1: discretionary security protection
  - Class C2: controlled access protection
- Division D: minimal protection

Source: INPUT

Vendors will need to take a more cautious approach to Orange Book standards in evaluating federal computer security in the current market. While the standards emphasize access control and confidentiality, such features as integrity and availability, more relevant to civilian agencies and private industry, are not weighed as rigorously. As an alternative

© 1995 by INPUT. Reproduction Prohibited.

approach to meet this need, NIST is developing a process called the Trusted Technology Assessment Program (TTAP), which resembles the United Kingdom's Commercially Licensed Evaluation Facilities (CLEF) program.

The European Community follows the Information Technology Security Evaluation Criteria (ITSEC), or White Book, developed by France, Germany, the Netherlands and the U.K., and published in 1991. Differing criteria for U.S. and European markets make security products more expensive to develop, test and bring to market for vendors. Consequently, NIST and NSA proposed new criteria to promote international coordination, and to improve Rainbow Series criteria and better address commercial requirements. Rainbow Series is a publication produced by the NCSC Technical Guidelines Program in support of the Trusted Computer System Evaluation Criteria requirements. These proposed "Federal Criteria," published in draft form in December 1992, were subsumed into an international effort in 1994.

The U.S., Canada and the European Community have drafted an international standard, the Common Information Technology Security Criteria, or "Common Criteria," incorporating experience from the Rainbow Series, ITSEC, and the Canada Trusted Computer Product Evaluation Criteria. Debate continues over the participation of Japan, Australia and other countries, and over the limited participation of the private sector.

The Computer Systems Security and Privacy Advisory Board discussed several major issues related to the security and privacy of sensitive but unclassified information in federal computer systems and those operated on behalf of the federal government. Among the most important, during 1994, were:

- Cryptographic Key Escrowing Procedures
- Alternative Key Escrow
- Security in the NII.

The draft Common Criteria were scheduled for review and discussion in 1995.

B
Market Structure

The federal computer security market can be broken out into various distinct segments reflecting the specialized areas of activity. They are:

© 1995 by INPUT. Reproduction Prohibited.

1. Professional services
    a. Consulting
    b. Education and training
    c. Software development
        i. Security software products
        ii. Computer security equipment.

Professional services include INPUT's three delivery submodes:

Consulting services include feasibility studies, requirements analyses, risk analyses, security plans and system audits. As with the Computer Security Act requirement for new security plans, it is expected that the requirement for periodic review of security and correction of deficiencies in Appendix III of OMB Circular A-130 will provide opportunities for consultants to assist agencies. The Architect-Engineer services of JAYCOR address physical and technical information security solutions. Integration services are provided by firms as diverse as Wang Federal Systems, and Booz Allen & Hamilton's consulting services range from policy development to the application and integration of security products. Other examples include BBN's Internet Managed Security Service and UNISYS' range of network engineering services.

Education and training continue as important components of this market, because Appendix III will require awareness and training of both agency employees and contractors. An OPM final ruling on the Computer Security Act in 1991 continues to require agency training for federal users and managers of computer systems used to process sensitive information.

Education and training are among the support services offered by systems integrators and are available from a range of professional services firms, such as Axent, which provides security training for all levels of personnel in addition to product-specific training. Education and training often are provided through, or in conjunction with, security product vendors teamed with professional services firms.

Software development includes trusted application development and other special efforts to enhance security at particular systems, locations or agencies. Modifications to standard products to create custom security solutions are part of this submode. Software development services are available from such organizations as UNISYS software engineering, and the TMACH system developed by Trusted Information Systems (TIS) is currently undergoing B3 (Exhibit III-2) evaluation by National Computer

© 1995 by INPUT. Reproduction Prohibited.

Security Center (NCSC). TIS provides other professional services ranging from system security analysis to awareness and training programs.

Security software products include commercially available product which is intended primarily to enhance automated information system security. It excludes general purpose operating systems and applications that incorporate standard security features, although software created specifically for security is included. The DEC MLS+, a secure UNIX operating system from Digital Equipment Corporation, and the Trusted Oracle 7 database management system are both MLS products that are B1 evaluated by the NCSC. In the category of encryption software, Entrust from Nortel and TECSEC's VEIL provide tools for data encryption and key management in applications ranging from enterprise networks to cellular and satellite communications.

Computer security equipment includes processor-based equipment used to protect automated information systems and Tempest-shielded processors and peripherals. Hardware providing physical protection, such as fire protection systems and electronic locking systems are excluded. The AS/400 computer system from IBM presents an integrated security solution, embedded in its OS/400 operating system and inaccessible to change by users, that is typically obtained through hardware-based system acquisition. Similar security solutions range from the TS 21 BLACKJACK secure facsimile from GKI to the FORTEZZA Cryptographic PCMCIA card from SPYRUS and National Semiconductor. Harris Computer Systems offers a variety of hardware-based security products evaluated B1 by NCSC, including the CyberGuard Firewall and Night Hawk router, gateway and network server computer systems.

The federal computer security market includes many products and services operating in classified environments. Information on acquiring these products is classified, preventing development of market sizing data and forecasts. Accordingly, INPUT has not covered them in this section or included them in the market forecast section, following.

NSA's MISSI is a program designed to make available an evolving set of security solutions that include MLS up to Top Secret/SCI. MISSI is providing interoperable security solutions for the Defense Information Infrastructure (DII), and addressing customer requirements for constituent programs such as the DMS, awarded to prime contractor and integrator Loral Federal Systems. MISSI building block products cover the security of workstations and networks, and include the FORTEZZA Crypto Card family of products and FORTEZZA-ready software applications. FORTEZZA Plus, to be utilized with high assurance guards, is intended to be sufficient for securing classified information.

© 1995 by INPUT. Reproduction Prohibited.

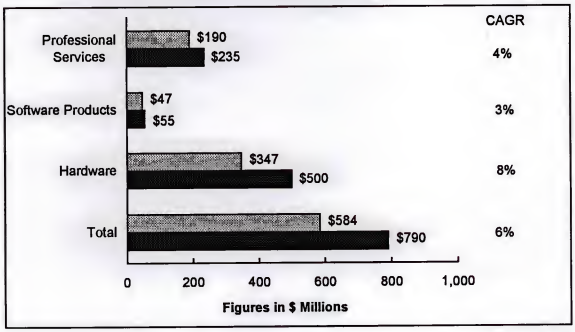
C
Market Forecast

The federal computer security market will grow from $584 million in FY 1995 to $790 million in FY 1999 at a CAGR of 6%. Accounting for inflation, this could be considered a slow market. Recent emphasis on expanding security requirements growing out of increased networking provides an improved growth expectation. Further impetus comes from the embedded nature of many security solutions, including those found in classified environments and integrated security not itemized separately for many IT budgets.

As indicated in the previous section, the federal computer security market includes professional services and the software products and equipment that operate in an unclassified environment. The combined forecast for the segments of this market is pictured in Exhibit III-3. The addition of classified applications probably will expand these numbers significantly. The lack of publicly available budget information, however, mandates the exclusion of this portion of the federal security market from this forecast.

Exhibit III-3

Federal Computer Security Market, FY 1995–2000



Source: INPUT

1. Civilian Market

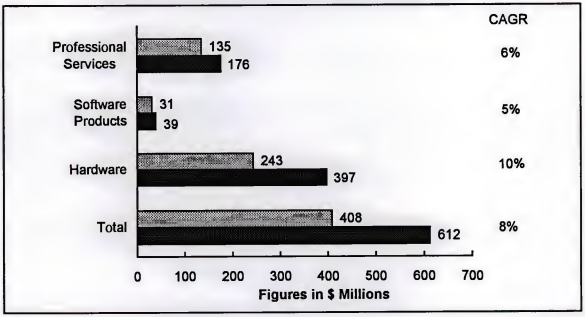
In a survey of user and vendors performed by INPUT for the 1992 Security Report, respondents were asked for their opinions on the differences between the civilian and defense markets for computer

© 1995 by INPUT. Reproduction Prohibited.

security services and products. Certain agencies, then as now, stand out as having the greatest emphasis on information security on the civilian agency side. The Treasury Department and the Department of Justice have the most stringent requirements, while scientific agencies, charged with sharing technical information, are at the other end of the scale. In between are social service agencies responsible for electronic delivery of services to the citizen. The relative robustness of this market is led by hardware, its largest segment and fastest growing element. The forecast for the civilian subsegments of the federal computer security market is expressed in Exhibit III-4.

Exhibit III-4

Civilian Computer Security Market, FY 1995–2000



Source: INPUT

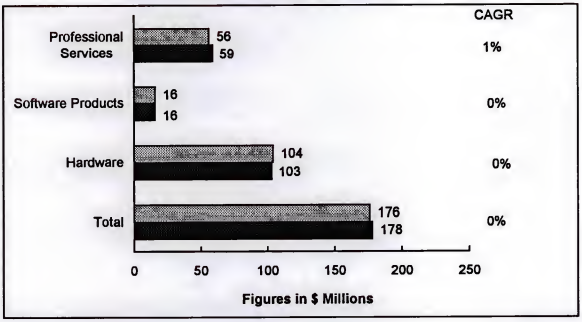
2. Defense Market

The defense agencies, from the vendors' perspective, appear more likely potential buyers for computer security products and services. Vendors are well known at some agencies and are familiar with defense agencies' automated information systems. The potential of this market, however, is mitigated by a 1% CAGR which, when inflation is considered, actually represents a decline. The defense share of total computer security budgets declines from 30% to 26% of the total during the period of INPUT's forecast. Exhibit III-5 displays the forecast for the defense market.

© 1995 by INPUT. Reproduction Prohibited.

Exhibit III-5

Defense Computer Security Market, FY 1995–1999



Source: INPUT

A comparison of the civilian and defense markets highlights stricter and more numerous standards and requirements imposed on defense agencies that are not applicable to their civilian counterparts. These standards and requirements in turn enhance vendor opportunities to provide customized hardware, software and integrated solutions for information security installations.

The overall federal IT market is determining, in part, the viability of the federal security market. Both market size and complexity are driven by the extent to which agency program managers include security requirements in their solicitations. The proposed Appendix III to OMB Circular A-130 requires controls to be established to assure adequate security for all information, either processed, transmitted or stored, in federal automated information systems. Management controls are emphasized, with both technical and operational controls and links to user behavior. Therefore, solicitations that place an emphasis on key management controls, shown in Exhibit III-6, will spur the need for products and services.

© 1995 by INPUT. Reproduction Prohibited.

Exhibit III-6

Key management controls

- Assigning responsibility for security
- Security planning
- Periodic review of security controls
- Management authorization

Source: INPUT

If OMB enforces the Computer Security Act requirement for annual security reviews, professional service firms will benefit from significant opportunities arising as a consequence. Conversely, if these reviews devolve into a paperwork exercise, little in the way of agency resources will be applied to the effort.

Although viruses and malicious code receive much media attention, NIST has stated that they are not the major problem. Rather than focusing narrowly on firewall and encryption solutions to Internet- and network-related security problems, NIST is stressing the need for a risk assessment-based management approach, much the same as that of OMB. Consequently, the market for professional services opportunities might grow at the expense of software-based solutions. Currently, the overall trend is for comparable growth in these two segments.

In segmenting the federal computer security market, an examination of current market issues is instructive:

Processing Services. In contractor-operated agency information processing services, computer security takes several forms in both contractor-owned and agency-owned facilities. The FAA CORN program is operated by EDS at facilities owned by the contractor, as is HUD HIIPS, by Lockheed Martin. CSC, on the other hand, runs NASA PRISM at government-owned facilities, and the USCS Springfield (Virginia) Data Center is operated by an 8(a) contractor.

Professional Services. Federal government spending on professional services support to meet information security needs is assured. The Computer Security Act requires appropriate training for selected personnel. The pending Appendix III to OMB Circular A-130 will, in some form, require the establishment of agency computer emergency response teams, link the oversight of federal computer security activities more closely to Federal Managers Financial Integrity Act (FMFIA) oversight, re-orient federal security programs to better respond to technological change, and require agencies to adopt a minimum set of management controls. Although the oversight agencies will be active in

© 1995 by INPUT. Reproduction Prohibited.

these areas, consulting support will continue to be required for evaluation and audits, as well as for upgrading information security activities.

The DISA Center for Information Systems Security (CISS) contract gives Computer Science Corporation (CSC), SAIC, and Merdan Group responsibility for a full range of information systems security solutions, including MISSI technology and DoD Goal Security Architecture. The DISA World Wide Military Command and Control System (WWMCSS) prime contract is held by Wang Federal Systems (formerly HFSI), an integrator working on the development of compartmented-mode workstations (CMW) for DoD, IRS, HHS and commercial users.

Software Products. The availability and functionality of software products and solutions continues to grow unabated. In the areas of information and network security, continuing attacks on internetworked systems are spurring development of this market as awareness rises with media publicity. A proliferation of Commercial Off-The-Shelf (COTS) products is finding its way into the federal market, even as NIST and NCSC continue to add trusted products and solutions to the Evaluated Products List (EPL).

Secure network management systems, based in PC software, are available from TimeStep to provide enterprise-wide security management. Software is available from GTE for complete electronic key management and, in conjunction with switching hardware systems, for securing Asynchronous Transmission Mode (ATM) networks. An overview of Rural Service Area (RSA) licensed products reveals virtually every major software publisher, and includes MS Windows, Apple Computer and Novell operating systems software.

Computer Equipment. Specialized computer equipment, as outlined in the previous section, forms the most significant component of the federal computer security market. Much of this equipment is listed on NSA's Preferred Products List (PPL). However, the PPL has been criticized as being too lax and the Tempest program, established in the 1950s, provides testing and endorsement for security products used almost exclusively to protect classified information. The emergence of an international standard—the Common Information Technology Security Criteria ("Common Criteria")—incorporating experience gained from the Rainbow Series may replace existing standards. The commercial influence, even if not incorporated, will see access control and confidentiality balanced by integrity and availability as security features more appropriate to open and networked computer systems.

Motorola's Caneware secures data networks with Tempest-rated equipment and secure operating systems utilizing accepted encryption standards. The Sidewinder from Secure Computing Corporation is a

© 1995 by INPUT. Reproduction Prohibited.

secure server and gateway providing firewall protection on Internet access, and meets DES and FORTEZZA standards.

Telecommunications. Networks were discussed briefly in preceding sections. A similarity of communications functions justifies the inclusion of LANs and WANs in the category of telecommunications. Use of these networks has grown considerably in the federal market, with a concurrent increase in the potential for security breaches, driving the market for software- and hardware-based protection against malicious code and intrusion. The widespread and growing use of E-mail and the Internet is extending the market for security products targeted at information networks.

Secure communications can be found in hardware offerings ranging from Rockwell's SEC*SAT STU III-capable satellite voice terminal to Motorola's KG-189 SONET encryptor, developed in conjunction with Nortel and capable of OC-48 (2.5 Gbps) communication rates.

Electronic Data Interchange (EDI). The NPR initiative and reinvention issues are stimulating greater use of electronic commerce to achieve agency objectives. As EDI becomes more widespread, the potential for security violations increases, a concern for both agencies and vendors. In its current survey of the federal computer security market, INPUT asked about the impact of security policies and regulations on electronic commerce initiatives, which is discussed in the following chapter. In addition to EDI, Public Key Encryption (PKE), for digital signature and message authentication, EFT (electronic funds transfer), and EIE (electronic information exchange, or E-mail) are increasingly relied upon in the use of networks. Thus the need for encryption tools remains strong with the availability of ever-increasing computing power.

A consortium of technology companies, CommerceNet, was formed to facilitate open, secure, Internet-based electronic commerce. Fischer International has created a workflow software program integrating EDI and digital signature support for security. Templar software from Romulus enables secure EDI and incorporates, as the two previous applications, the RSA Public Key Cryptosystem for secure encryption and authentication.

D
Federal Market Pressures

Competing market pressures, shown in Exhibit III-7, are driving this market. The Computer Security Act of 1987 exerted positive pressure, requiring training and development of security plans and, in the process, raising awareness and encouraging greater understanding and

© 1995 by INPUT. Reproduction Prohibited.

appreciation of security issues at federal agencies. The pending Appendix III of OMB Circular A-130 will continue this process with its requirement for controls to assure information security and its emphasis on the management of risk rather than its measurement.

Exhibit III-7

Federal Computer Security Market Pressures

- Encouraging computer security issues
  - Legislative mandate
  - Policy initiative
  - Increased Internet access
  - More information sharing
  - Open network architecture
  - Greater agency awareness
  - Publicized attacks and incidences
- Discouraging computer security expenditures
  - Budget constraints
  - Competing priorities
  - No follow-up legislation

Source: INPUT

Following the trends in the private sector, federal agencies are moving computing power to end users through networked PCs and client/server architectures. Requirements are growing for more open systems and shared information, driving standards for interoperability and compatibility. Greater ease of use is a requirement, and software features reduced human effort. These same trends, however, tend to promote the risk of security violations. Open network architecture and information sharing initiatives tend to create threats to the security of automated information systems, and viruses and malicious code seem to be on the rise, costing agencies increasing amounts of resources to correct.

On the positive side, concerted effort at NIST, NCSC and NSA is dedicated to improving computer security. The challenges raised by rapidly evolving information infrastructures are being addressed and met.

Negative pressures, as indicated in Exhibit III-7, are working to discourage growth of the federal computer security market. By far the most significant is budgetary; limited funds, shrinking budgets and competing priorities all work to restrain the expansion of this market. Because computer security is supposed to be included in overall system authorizations, agencies seldom receive funds specifically for it. Thus, computer security is left to compete with new program funding.

© 1995 by INPUT. Reproduction Prohibited.

Another obstacle is the lack of follow-up legislation. While OMB is moving to revise security responsibilities with respect to the Computer Security Act, little has been done in Congress to improve federal computer security.

E
Laws, Regulations and Policies

The framework for security in the federal government can be viewed as a pyramid, with laws enacted by Congress at its apex. Then come policies from OMB, followed by guidelines, regulations and standards from GAO, GSA and NIST. The foundation consists of departmental directives and other automated information system-specific guidelines, policies and procedures. The following laws form the basis of the federal computer security hierarchy.

- The Accounting and Auditing Act of 1950 (31 USC 65). The act establishes policies for accounting for federal assets, and auditing standards for federal administrative systems.
- The Brooks Act (PL 89-306), 1966. The act defines the basic roles of GSA, NIST and OMB relative to data processing, and consolidates all ADP procurement authority under GSA.
- The Privacy Act of 1974 (PL 93-579). The act provides for the protection of information contained in federal information systems related to individuals, and prescribes penalties and remedies relative to disclosure.
- The Federal Managers' Financial Integrity Act (PL 97-255), 1982. The FMFIA addresses waste, fraud and abuse in financial/accounting systems and gives GAO standard-setting authority.
- OMB Circular A-130, Management of Federal Information Resources, 1985. This document binds the first four laws to automated information system security and control, and comprehensively defines the concept of computer security and its applications.
- The Computer Fraud and Abuse Act of 1986 (PL 99-474). The act establishes computer-related crime as a separate offense, and provides penalties.
- The Computer Security Act of 1987 (PL 100-235). The act defines the computer security roles of NIST, NSA, OMB and the Office of Personnel Management (OPM), and requires development of security plans, periodic reviews and provision of computer security awareness training.

© 1995 by INPUT. Reproduction Prohibited.

- OMB Circular A-130 Appendix I, Federal Agency Responsibilities for Maintaining Records About Individuals, June 25, 1993. This revision concerns information exchanges with the public.

- OMB Circular A-130 Appendix II, Federal Agency Management Practices for Information Systems and Information Technology, July 25, 1994. This revision concerns agency investments in information technology that improve service delivery to the public and lower the cost of programs administration.

Along with the revision of OMB circulars, GAO standards and guidelines, the GSA FIRMR and NIST standards and guidelines were extended to accommodate the growing federal use of computers, and to address specifically the problems associated with automated information processing.

F
Key Federal Agencies

In addition to Congress, a number of federal agencies play active roles in computer security. This section covers the activities of some of these agencies.

1. General Services Administration

GSA plays a minor role in the regulation of computer security. Its responsibility to issue policies and regulations is in the following areas:

- Physical security of computer rooms, consistent with NIST guidelines

- Agency procurement requests for computer equipment, software and related services, including security

- Procurements made by GSA to meet user agency-established security requirements.

The Federal Information Management Regulation (FIRMR) issued by GSA provides guidance for acquisition and management of information resources. 41 CFR, Ch. 201 covers security for information systems under development. The FIRMR, paralleling OMB Circular A-130, requires a security program that:

- Ensures the safeguarding of sensitive data under all conditions

- Provides for operational reliability of ADP and telecommunications systems

© 1995 by INPUT. Reproduction Prohibited.

- Provides asset integrity for prevention of loss from physical hazards.

GSA's Office of Technical Assistance (OTA) and its Federal Systems Integration and Management Center (FEDSIM) provide a range of services to other federal agencies. Vested by the Brooks Act with exclusive authority to provide for the procurement of ADPE, with certain specified exceptions, GSA established the FEDSIM program. Agencies enter into interagency agreements under the Brooks Act, exempt from the Economy Act (31 USC 1535), and may obligate funds without fiscal year limitation. GSA also has interpreted FIRMR 201-20.305 as not requiring agencies to obtain a delegation of procurement authority (DPA) when contracting through FEDSIM. Among OTA/FEDSIM service offerings is information technology system security, including:

- Security program and procedural development
- Risk analyses, security audits, application reviews and vulnerability assessments
- Contingency plans.

2. Office of Management and Budget

OMB is directed, under the provisions of the Computer Security Act of 1987, to issue regulations prescribing the scope and procedures of training to be provided federal employees. Guidelines have been published by OMB for agency use in preparing computer security plans, and require documentation of security awareness and training programs. Continuing revisions to Circular A-130 are updating security practices required of agencies, as OMB continues to review agency policies, practices and programs relating to the security, protection, sharing and disclosure of information in automated systems.

3. National Security Agency

Established by presidential directive in 1952, NSA is a separately organized agency within DoD. In 1984, it was charged with responsibility for computer security under another presidential directive. NSA has the following responsibilities:

- Prescribing certain security doctrines, principles and procedures for the federal government
- Organizing and coordinating research and engineering activities of the federal government, in support of NSA's assigned security mission
- Operating the NCSC

© 1995 by INPUT. Reproduction Prohibited.

- Evaluating and certifying security products under TCSEC for the EPL.

NSA and NIST entered into a Memorandum of Understanding regarding the security of sensitive data. The Computer Security Act specifies that the technical advice and assistance of NSA shall be called upon when appropriate. NSA and NIST jointly reviewed computer plans submitted by federal agencies as required by the Act, and returned them with comments and suggestions.

The influence of NSA on the federal computer security market is most visible in its establishment of the hierarchy of computer security ranking defined in the DoD TCSEC (Orange Book). The NCSC evaluates and certifies information security products according to the levels listed in Exhibit III-2.

4. National Institute of Standards and Technology

NIST, originally the National Bureau of Standards (NBS), is an agency of the Department of Commerce. The NIST information security mission is to:

- Develop and maintain security standards
- Provide advice and guidance to federal agencies in the use of standards
- Assist federal agencies in systems development efforts
- Provide assistance to the private sector in the use of standards
- Conduct computer security-related research and studies.

NIST, along with NSA, establishes computer security standards for civilian agencies and reviews computer security plans submitted by federal agencies. Working with DoD, Department of Justice (DOJ) and NSA, NIST coordinates agency responses to security incidents and maintains a clearinghouse for security issues.

The CSL operates under the direction of NIST to conduct research and maintain liaison with industry. An organizational chart for the Laboratory is shown in Exhibit III-8. NIST, in conjunction with NCSC and NCL, hosts the annual National Computer Security Conference. It also formed and hosts the Computer Systems Security and Privacy Advisory Board, created by the Computer Security Act and staffed by directors from private industry and academe, as well as the federal government. The Board is charged by the Act with the following objectives and duties:

- Identifying emerging security issues

© 1995 by INPUT. Reproduction Prohibited.

- Advising NIST and the Secretary of Commerce on security and privacy issues
- Functioning solely as an advisory body.

The Board consists of a chairman and twelve members, and is made up as follows:

1. Four members from outside the federal government eminent in the computer or telecommunication industry, with at least one representative from a small or medium-sized company.

2. Four members from outside the federal government eminent in computer or telecommunication technology or related disciplines who are not employed by computer or telecommunication equipment manufacturers.

3. Four members from the federal government, including one from NSA, who have experience in computer systems management and computer security and privacy.

The Board reports through the Director of NIST to the Secretary of Commerce, to the Directors of OMB and NSA, and to appropriate congressional committees.

Exhibit III-8

Computer System Security and Privacy Advisory Board

Chairman: Willis H. Ware

The RAND Corporation

Term expires Sept. 1996

Sept. 1995	Sept. 1996	Sept. 1998	Sept. 1999
Cris R. Castro KPMG Peat Marwick	Sandra Lambert Citicorp	Charlie C. Baggett, Jr. NSA	Joseph Leo USDA
Gaetano Gangemi Wang Laboratories	Bill Whitehurst IBM Corporation	Genevieve M. Burns Monsanto Corporation	
Henry Philcox IRS (retired)		Randolph Sanovic Mobil Corporation	
Stephen T. Walker Trusted Information Systems		Steven A. Trodden DVA	
		Linda Vetter Oracle Corporation	

Source: INPUT

© 1995 by INPUT. Reproduction Prohibited.

IV

Federal User Requirements and Trends

This section describes the results of INPUT's current survey of federal agencies as well as other agency information reflecting requirements and trends in security of automated information systems. Agency responses showed a wide mix of opinion on present and future needs for information security. Although all agencies agreed on the need for information security, the most important selection criterion was ease of implementation. While secure network capabilities, password systems, product price and training features received strong marks, the results indicate some flexibility for vendors in responding to federal security needs. The market still is characterized by a lack of clear definition. More than half of agency respondents viewed past and current vendor efforts as either very satisfactory or satisfactory. This result shows an improvement in vendor performance in increasing agency confidence during the three-year period since INPUT's previous report on this market. Agency responses indicated improvement made in the areas of price, software offered and encryption experience. The challenge of overcoming budget constraints and enhancing market penetration will require vendors to market heavily.

A
Security Plans: Implementation and Compliance

1. Purpose of Security Plan

During the current survey of federal agencies, INPUT asked what respondents believed was the purpose of the security plan implemented by their agency. In its past survey, INPUT examined security measures adopted pursuant to the Computer Security Act of 1987. Identification of sensitive systems, security plans completed, and security plans implemented were the measures, with the latter affirmed by only 41% of respondents at the time of the survey. Under the Act, agencies were

© 1995 by INPUT. Reproduction Prohibited.

required to submit security plans to NIST, and implementation has been subject to OMB review.

The current survey, its first eight questions directed at security plans, guidelines and controls, found responding agencies in compliance with the basic requirements of the Computer Security Act. In addition, security awareness and training requirements of the Act, notable for agency shortcomings found by NIST and NSA at the time of the past survey, are being addressed by the agencies. As noted in Exhibit IV-1, improving awareness drew the second largest positive response from respondents, underscoring agency responses to the requirements of the Act.

Exhibit IV-1

Purpose of Security Plan

	Number of Responses	Percent of Respondents
Respond to Requirements of Law	16	67
Improve Awareness	15	63
Set Policy for Behavior	13	54
Identify Solutions	8	33
Other	7	29

Total responses = 24 *Source: INPUT*

Exhibit IV-1 summarizes the results of the survey of the purpose of security plans implemented by agencies. Most agency respondents provided more than one answer. All participants in the agency specified the need for network security, an unusual level of agreement among agency respondents. Two-thirds of the participants specified the need to respond to requirements of law. Improving awareness of computer security requirements also received high ratings. Setting policy for behavior was the only other response given by more than half of the agencies surveyed. These responses suggest that the agencies are fully aware of and are following the rules set forth by the Computer Security Act of 1987 but are not necessarily observing the full intent of the act. Identifying solutions to security problems was named by only a third of respondents and other purposes cited reflect the rules of the Act, including protecting information assets and appropriate planning. Giving a security profile and keeping GAO and oversight agencies at bay were also noted.

Budget issues related to security emerged in these responses, with security plans utilized for prioritizing the application of limited resources based on assessment of risk, and budget justification for certification and accreditation.

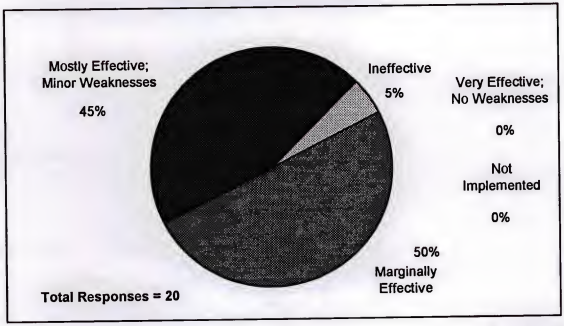
© 1995 by INPUT. Reproduction Prohibited.

2. Effectiveness of Security Plan

Exhibit IV-2 illustrates the respondents' views of the effectiveness of agency implementation of security plans. Of twenty respondents to this question, fully half rated security plan implementation as being marginally effective. One saw implementation as ineffective and the balance reported mostly effective, with minor weaknesses. This result suggests a continuing need to address the intent, as well as the letter, of the Computer Security Act.

Exhibit IV-2

Effectiveness of Security Plan



Source: INPUT

While compliance has climbed from the time of INPUT's past survey, federal agencies clearly can benefit from vendor support in security plan and policy development. Agency program managers steadily are gaining experience in defining security requirements and developing plans. However, more rigorous security plans and training are continuing to be required of federal agencies as the nature of information security evolves. Furthermore, as agencies move closer to compliance with all of the provisions of the Computer Security Act, new requirements are emerging from the update of Appendix II of OMB Circular A-130.

3. Security Plan Coverage

The question "What does your security plan cover?" gave respondents a choice of 24 topics taken from security plans and past surveys. The results show password control drawing the greatest number of responses,

© 1995 by INPUT. Reproduction Prohibited.

underscoring agency concern for user access control issues. The second and third highest responses, to network access and system access, respectively, reemphasize this concern for access as central to security planning. Viruses and malicious code tied for third, and disgruntled employees and network hackers, with equal fourth-place responses, underscore the concern for human factors that has come to preeminence in information security planning. Exhibit IV-3 pictures the range of coverage issues and indicates the greater relative concern for desktop equipment rather than for the mainframes and minicomputers found in data centers.

Exhibit IV-3

Security Plan Coverage

	Number of Responses	Percent of Respondents
Password Control	17	71
Network Access	16	67
System Access	15	63
Viruses and Malicious Code	15	63
Disgruntled Employees	14	58
Natural Disasters	14	58
Network Hackers	14	58
Computer Ethics	13	54
Internet Access	13	54
Micro	13	54
Proprietary Information	13	54
Software Use	13	54
Client/Server	12	50
Laptop	12	50
Theft of Equipment	12	50
Employee Handbook	11	46
Information Leaks	11	46
Insufficient Security	11	46
Data Center	11	46
Terrorism	11	46
Document Control	10	42
PBX Fraud	7	29
Other	7	29
Industrial Espionage	6	25

Total Responses = 24 *Source: INPUT*

© 1995 by INPUT. Reproduction Prohibited.

Lower on the scale, the threat of terrorism, a dramatic but infrequent occurrence, and PBX fraud, an underpublicized but costly security violation, were cited by fewer than half of respondents. Other security concerns included high-tech crime investigation, audit trails, physical protection of assets, personnel security, and acquisition security. A range of hazards, both natural and man-made, complete the list of vulnerabilities impacting the accuracy, integrity and continuity of computer operations.

4. Review of Security Controls

Security controls, including management, operational, personnel and technical controls, were addressed in the question "Does your agency periodically review security controls?" Respondents were given choices of both "upon significant system modification" and "every three years." Both were affirmed by a large majority, with the former scoring 90% and the latter 88%. Given that the security of automated information processing systems degrades over time, as technology evolves and people and procedures change, formal management reviews and independent audits have become a necessity. Indeed, for some high risk systems, three years may be too long.

5. Written Authorization for System Use

Authorized processing is an important element of management control, addressed in the question "Is system use authorized in writing based on the security plan?" The categories of "before beginning or significantly changing processing" and "every three years" drew fewer responses than the preceding survey question, indicating a lower level of this quality control activity. Of those responding, 74% said yes to the first part and 85% to the second. The process of authorization, a responsibility of management and not security staff, sometimes is referred to as accreditation. Some agencies perform accreditation reviews periodically, enabling a management accreditation, or authorization to process.

B
Directives and Guidelines

Federal agencies must move rapidly toward implementation of information security measures in order to comply with already established and evolving security guidelines. Failure to maintain adequate security controls in government computer systems will have increasingly important consequences. Federal agencies are becoming increasingly dependent on automated information systems to process and maintain a range of sensitive and mission-critical information. With decentralized computer systems and greater dependence on automated information processing, government information resources are becoming increasingly vulnerable.

© 1995 by INPUT. Reproduction Prohibited.

The Computer Security Act specifies the responsibilities of NIST for developing security guidelines for, and OMB for review and evaluation of agency policies, practices and programs pertaining to information security. Cited frequently in INPUT's past survey, OMB Circular A-130 contains the security guidelines relevant to the development of automated information systems. The present survey asked which directives and guidelines were used, in addition to Appendix III of A-130, a proposal designed to reorient the federal computer security program to better respond to a rapidly evolving technological environment.

1. Directives and Guidelines Used

Eighty-eight percent of agency respondents cited departmental directives as the most used security guidelines, as shown in Exhibit IV-4. Responses fell off abruptly to the 38% using NIST Bulletins, NIST National Reports (NISTRs) and Special Publications.

Exhibit IV-4

Directives and Guidelines Used

		Number of Responses	Percent of Respondents
1	Departmental Directives	21	88
2	NIST Bulletins, NISTRs, Special Publications	9	38
3	Computer Security Act of 1987	8	33
4	DOD 5200.08-STD	8	33
5	FIPS	8	33
6	OMB Circulars (except A-130) and Bulletin	7	29
7	Rainbow Series and NSC TSRs	7	29
8	NTISSI/NTISSP	5	21
9	Privacy Act	4	17
10	Executive Orders	3	13
11	FIRMR	3	13
12	FMFIA	3	13
13	Entire 28 CFR	1	4

Total responses = 24 *Source: INPUT*

A notable survey result shown here is the size of the responses acknowledging the roles of NIST and OMB. Agency perceptions are of security guidelines originating within departments and not from a higher government-wide source.

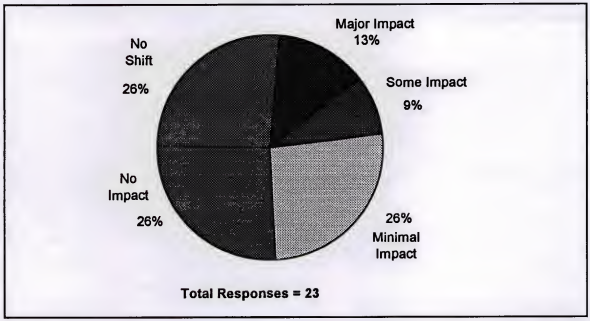
© 1995 by INPUT. Reproduction Prohibited.

2. Impact of Appendix III to OMB Circular A-130

The shift of emphasis from the measurement of risk to the management of risk, a significant feature of the proposed Appendix III of OMB Circular A-130, is the basis for the survey question illustrated in Exhibit IV-5. Agencies were asked to rate the impact of this change on their security plans and operations, and responses reflected a range from a proactive view of the revision to denial of any present applicability.

Exhibit IV-5

Impact of Appendix III to OMB Circular A-130



Source: INPUT

Intended to guide agencies in maintaining and improving information security as they become increasingly reliant on an open and interconnected NII, the proposed revision stresses management controls such as individual responsibility, awareness and training, and accountability, rather than technical controls. It aims to revise government-wide security responsibilities to be consistent with the Computer Security Act.

C
Future Computer Security Measures

More rigorous security programs and measures will be needed by federal agencies in the future for the protection of automated information systems. Protecting the integrity and privacy of information resources in a more uniform manner across agencies is a requirement for agency security plans in the revision of Appendix III of OMB Circular A-130, which takes into account the provisions and intent of the Computer Security Act. As agency

© 1995 by INPUT. Reproduction Prohibited.

program managers gain experience in developing and implementing security plans, all federal agencies should move closer to compliance with all of the provisions of the Act.

Agency responses to questions about computer security measures planned for the future are illustrated in Exhibits IV-6 through IV-10. In asking which computer security products and services agencies planned to inquire, INPUT segmented the products and services, as reflected in the above-cited exhibits, and identified planned acquisitions within two years, and in three to five years.

1. Acquisition of Administrative Services

Administrative services, reflected in Exhibit IV-6, highlighted agency interest in security education, with 79% of respondents checking within 2 years and 29% in 3 to 5 years. Responses within 2 years dropped quickly to 46% for risk assessment/analysis and only 42% for contractor assistance for preparation of security plans and other contractor administrative support, while procurement of these services in 3 to 5 years is checked at the same level as education.

Risk analysis, an evaluation of system assets and vulnerabilities made to establish estimates of loss, is based on cost and probabilities of occurrence or ranking of categories of risk of security incidents. An element of security planning affecting all agencies, its significance in the revision of OMB Circular A-130 is not reflected in the level of response found.

Exhibit IV-6

Acquisition of Administrative Services

	Within 2 Years	3 to 5 Years
Security Education	19	7
Risk Assessment/Analysis	11	7
Contractor Assistance for Preparation of Plans	10	6
Other Contractor Support	10	7
Regular Security Audits	8	5
Decentralized Security Administration	4	3

Total responses = 24 *Source: INPUT*

Regular security audits within 2 years were selected by only a third of respondents, an unexpected finding given the emphasis on periodic review of security controls found in guidelines and directives affecting federal agencies.

© 1995 by INPUT. Reproduction Prohibited.

2. Acquisition of Hardware

Projected hardware acquisitions, shown in Exhibit IV-7, rated communications security products the highest, at 75% within 2 years, reflecting agency concern for greater security in networked systems and open, distributed architecture. Secure telephones and workstations and other contractor security devices drew more frequent responses from the defense agencies, while interest in back-up power supply and on-line file backup was distributed more evenly across the federal government.

Exhibit IV-7

Acquisition of Hardware

	Within 2 Years	3 to 5 Years
Comunications Security Products	18	7
Secure Workstations	15	6
Secure Telephones	13	7
Other Contractor Security Devices	11	7
Back-up Power Supply	10	6
On-line Back-up Files	10	5
Separate Computer for Software Testing	7	3

Total responses = 24 *Source: INPUT*

As with administrative services, projected procurement of the various categories of security hardware was distributed more evenly in the 3 to 5 year period.

3. Acquisition of Physical Security

The category of physical security, as revealed in Exhibit IV-8, drew limited responses from agencies. In both the 2-year and 3-to-5-year time frames, the focus on management controls and the growing emphasis on managing risk, through assessment and analyses, underlies the declining interest in hardware solutions. Tangible assets, including physical facilities and systems hardware, concern a class of assets whose value in terms of replacement, restoration and penalty costs is lower than that of information assets.

© 1995 by INPUT. Reproduction Prohibited.

Exhibit IV-8

Acquisition of Physical Security

	Within 2 Years	3 to 5 Years
Computer Room Security	9	4
Off-site Storage of Back-up Files	9	4
Emission Control Devices	5	4
Tempest Products	5	3

Total responses = 24 *Source: INPUT*

Two trends in the security of automated information systems are illuminated here. Securing the information, rather than the channel, is evident in the evolution of guidelines and directives at federal agencies. As well, the move to software-based information systems security has had a concurrent impact on the relative standing of hardware solutions.

4. Acquisition of Software

The future implementation of software solutions to the challenges of securing automated information systems elicited the strongest responses among all categories of planned security measures. Exhibit IV-9 details the responses within 2 years, ranging from 92% for encryption software and the 88% for both access control software and antivirus software to the still significant 54% for automatic file backup. Only single sign-on at a 38% rate slipped below half of all responses, indicating some resistance to the concept.

Exhibit IV-9

Acquisition of Software

	Within 2 Years	3 to 5 Years
Encryption	22	5
Access Control Software	21	5
Antivirus Software	21	4
Network Access Control	18	5
Dial-up Port Protection	15	4
Message Authentication	15	5
Password Management	15	4
Secure Unix-based Products	14	3
Automatic File Backup	13	3
Single Sign-on	9	4

Total responses = 24 *Source: INPUT*

A remarkable consistency is reflected in the 3-to-5-year acquisition plans for software-based security measures. The mathematical nature of

© 1995 by INPUT. Reproduction Prohibited.

encryption drives the software-based implementation of this ubiquitous technology in increasingly open and internetworked systems, and protection of information assets through both access control and antivirus software applications supports the growth and importance of software solutions. Control of network access, identification and authentication, and password management are all important security measures in the view of respondents, reinforcing the strong market position of software-based solutions to the protection of information resources.

5. Acquisition of Other Security

Other security products and services, presented in Exhibit IV-10, related to system architecture and certification of security products drew a limited number of responses from a narrow range of agencies.

Exhibit IV-10

Acquisition of Other Security

	Within 2 Years	3 to 5 Years
Distributed System Security Architecture (DSSA)	7	3
NCSC-Certified Products	3	1
ITSEC-Certified Products	0	1

Total responses = 24 *Source: INPUT*

Defense agencies predominated in overall responses, both within 2 years and in 3 to 5 years. The only non-U.S. standards addressed in this survey, the European Economic Community's ITSEC, or European "White Book," were cited by a department with international concerns.

D
Implementation and Access

The implementation of security measures, as distinct from overall formal security plans, was addressed in the following series of survey questions. Access to automated information systems, by other government agencies and entities and by the public, was examined as well. In response to the question "Has backup and restoration of service capability been established?" 92% of respondents said yes. The total declined to 87% when agency representatives were asked if they believed there were cost-effective solutions to their security requirements. Contrasted with respondents' pessimistic views of budget levels, discussed in Section H of this chapter, this predominant view of available security solutions is a clear sign of market responsiveness to user needs.

Authorized interconnection with other systems was examined in the specific context of security controls on the other systems and their

© 1995 by INPUT. Reproduction Prohibited.

consistency with those for the system itself. The negative responses rose to one third, indicating a substantial weakness in management controls on interconnection and internetworking. The same ratio of negative answers appeared for the security of major applications, and extension of that same level to information shared outside the system. Although fewer responses were received, reflecting a subset of all agencies surveyed concerned with major applications, the concern for the security of internetworked information remains. A major application is one requiring special attention to security because of the risk and magnitude of potential loss from security incidents.

Public access subject to security controls was the topic of the final survey question in this series, examining in turn computer systems, major applications, and bulletin board services. When asked if security controls applied to public access, 100% of respondents affirmed this for the first two categories. Electronic bulletin boards were reported by 11% of agencies responding as being accessible to the public without adequate security.

E
Functional Requirements and Performance Criteria

There is a broad spectrum of functional security requirements that can be applied to information systems, ranging from relatively uncomplicated and inexpensive to technically challenging and very expensive. The use of logon identities and passwords is one example, and the other extreme is the A1 level of certification for verified design of trusted systems under TCSEC evaluation from NCSC. The selection of functional requirements can have significant impact on system costs, complexity, delivery schedules and performance.

1. Performance Criteria Priority

Identification of particular functional security requirements was made according to the numbers of respondents choosing high priority in the question "What priority has your agency assigned for the following performance criteria?" charted in Exhibit IV-11. Continued service drew the most responses, 83%, while access control and back-up and recovery provisions were tied for a close second. The distribution of responses highlights the risks and threats of greatest concern to federal agencies. The maintenance of continuity of operations is rated as number one, and the importance given backup and recovery underscores the priority respondents now place on protecting the accuracy, integrity and continuity of computer operations and information processing for mission-critical and sensitive systems.

© 1995 by INPUT. Reproduction Prohibited.

Exhibit IV-11

Performance Criteria Priority

Criteria	High	Low	None
Continued Service	20	4	0
Access Control	19	3	1
Back-up and Recovery Provisions	19	3	1
No Security Breaches	14	7	2
Physical Security	14	8	0
Other	0	0	0

Total responses = 24 *Source: INPUT*

Control of access includes user identification and authentication, which verifies the user's eligibility for accessing the system. Functional safeguards to assure limited and appropriate access to sensitive information and systems include passwords, encryption techniques and multilevel security operating systems.

Physical security requirements were cited by only 64% of respondents, down from 86% in the past survey by INPUT. These include limited or restricted access to data centers, remote sites, and the hardware of LANs and internetworked systems. Physical security is typically the least costly and easiest functional requirement to fulfill. However, it may be the least effective against the threats most concerning respondents, those based on unauthorized and typically electronic, or non-physical, access.

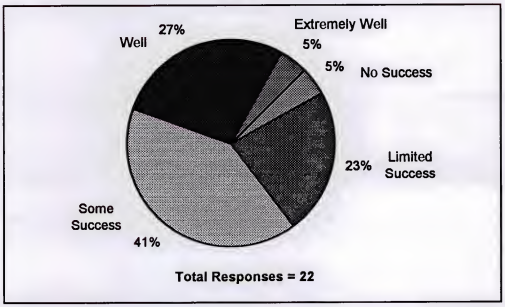
2. Success of Products in Meeting Current Criteria

Agency respondents evaluated the level of success attained by vendors in achieving current agency performance criteria. The degrees of success, based on agency experience, are shown in Exhibit IV-12. The levels ranged from extremely well, in five stages, through not successful at all, and were representative of a prototypical statistical distribution.

© 1995 by INPUT. Reproduction Prohibited.

Exhibit IV-12

Success of Products in Meeting Current Criteria



Source: INPUT

Forty-one percent of respondents viewed security products and services as achieving some success in meeting current criteria, and a total of 73% found vendors meeting this level or higher. Among this majority, some respondents suggested future improvements were needed to provide not only ease of implementation, but greater protection against unauthorized system access, viruses and malicious code, and unauthorized network access.

3. Selection Criteria for Security Products and Services

The relative importance of various criteria in the selection of security products and services is rated by agency respondents in Exhibit IV-13. Ease of implementation was most important, with secure network capabilities, password systems and the price of products and services achieving nearly equally high ratings. The technical complexity of many current security solutions is of real concern in the federal marketplace, while the growth of open and internetworked systems demands greater levels of security and access control than older, proprietary computer systems.

© 1995 by INPUT. Reproduction Prohibited.

Exhibit IV-13

Selection Criteria for Security Products and Services

	Criteria	1	2	3	4	5
1	Ease of Implementation	14	4	1	0	0
2	Secure Network Capabilities	13	5	1	1	0
3	Password Systems	12	4	3	1	0
4	Product/Service Price	12	7	1	2	0
5	Training Features	11	4	6	0	0
6	Vendor's Support Reputation	7	9	2	2	0
7	Encryption Features	7	6	6	0	0
8	Vendor's Federal Experience	0	4	11	4	0
9	Other: System Dependent	1	0	0	0	0

Total responses = 24 *Source: INPUT*

The issue of price has traded positions with vendor's support reputation since the past INPUT survey, with price gaining much more importance than support reputation lost in number of responses. A favorable reputation still carries weight throughout the federal government and a poor one, also passed on by word of mouth, is difficult to overcome. Federal experience, as in the past survey, was ranked least important, but still with a moderate rating, by survey respondents.

F
Acquisition Plans and Preferences

1. Acquisition Methods

Agency respondents were asked to comment on the planned methods of procuring information security products and services. Multiple responses were given to the types of acquisition methods preferred, as shown in Exhibit IV-14. Multiple replies indicate agency plans to employ more than one method, depending on particular security needs.

© 1995 by INPUT. Reproduction Prohibited.

Exhibit IV-14

Acquisition Methods

	Number of Responses	Percent of Respondents
GSA Schedules	14	58
RFPs for Specific Purchase	14	58
RFP for Requirement Contract	13	54
Purchase as Part of Other Procurements	13	54
Other	4	17
Most often used:		
RFP for Requirement Contract	6	
GSA Schedules	1	

Total responses = 24 *Source: INPUT*

While 58% of respondents expect to buy from the GSA Schedules, an equal share indicated agency use of RFPs for a specific purchase. Interestingly, the selection of both RFP for requirement contract and purchase as part of other procurements by 54% of respondents represented a leveling of acquisition method preferences over INPUT's past survey. The large increase in acquiring security products and services as part of other procurements indicates a burgeoning trend in government. The use of contracts such as DMS was mentioned by respondents, who also noted sole source selections and DoD-wide contracts as the preferred method of acquisition.

The questionnaire also asked respondents to indicate their most often used method of acquisition. Of those responding, 86% cited RFP for requirement contract, a growing trend among federal agencies observed in INPUT's past survey to be extending into the information security market. The GSA Schedules were selected by 14% as the most often used method of procurement.

2. Most Appropriate Vendor

Respondents were asked which type of vendor was preferred for providing computer security products and services for their agencies. Exhibit IV-15 shows the results, with multiple selection raising the total well above 100%. Software vendors again drew the greatest number of responses while hardware vendors moved from second to fourth place, as contrasted with the past INPUT survey. Again, the trend toward greater use of software-based solutions is supported by the response of federal security managers and policymakers.

© 1995 by INPUT. Reproduction Prohibited.

Exhibit IV-15

Most Appropriate Vendor

	Number of Responses	Percent of respondents
Software Vendors	9	38
Professional Service Firms	8	33
Systems Integrators	7	29
Hardware Vendors	4	17
Not-for-Profit Firms	3	13
Aerospace Divisions	2	8
Other	5	21

Total responses = 24 *Source: INPUT*

The agency preference for software vendors was supported by statements that these vendors are providing needed product support and are meeting a variety of agency security requirements with their products. Professional services firms and systems integrators both moved up, showing increasing agency preference for the technical support needed in many new security implementations. The flexibility offered by professional services firms in providing agencies with a range of services and options is in greater demand at the agencies. As security requirements and services are installed on more networks and open systems, the use of systems integrators is continuing to grow, a trend noted in INPUT's past survey.

3. Use of GSA Contractors

Agency representatives were asked their use of, or intent to use, GSA contractors. Of those responding, 63% answered in the affirmative. The following survey question sought to determine which contractor and why. The first, picked by multiple respondents, was the fee-for-service offerings of GSA's FEDSIM program in OTA. In addition to FEDSIM, complementary programs offered are the Federal Information Systems Support Program (FISSP) and the Federal Computer Acquisition Center (FEDCAC). Agency respondents cited acquisition support for contractor selection, requirements analysis, and RFP and technical specifications support as FEDSIM services utilized. Other contractors, and the reasons for their selection, included:

- Booz Allen & Hamilton - Computer security services
- Comdisco - Disaster avoidance, threat reduction
- Comsys - Security plans, training, risk assessment, procedural guidance

© 1995 by INPUT. Reproduction Prohibited.

- Interagency agreement - Risk assessment contract
- Mitre - "a lot"
- PRC - Computer security services
- Security Dynamics - Secured authentication tokens
- Technautics - Security plans, training, risk assessment, procedural guidance
- Troy Systems - Policy development, security plans, procedural guidance
- Unknown - lowest bidder.

G
Vendor Performance

The overall level of agency satisfaction with vendor performance characteristics was moderate for all factors in the current survey, paralleling the responses tallied in the past INPUT survey. The ratings given to each factor, shown in Exhibit IV-16, have a slightly greater range, 3.4 to 2.5, than those of the past INPUT survey at 3.3 to 3.1. Successful implementation moved up slightly from a 5-way tie at 3.3 to top the current ranking at 3.4.

Exhibit IV-16

Vendor Performance Ratings

Criteria	1	2	3	4	5
Successful Implementation	2	5	3	2	2
Support Experience	2	4	5	2	1
Staff Experience	2	4	3	2	3
Training Experience	2	2	5	3	2
Hardware Offered	2	3	1	4	1
Price	1	3	4	3	3
Software Offered	1	4	3	2	3
Delivery Schedule	0	6	4	3	0
Encryption Experience	0	2	5	3	3
Other: System Dependent	1	0	0	0	0

Total responses = 24 *Source: INPUT*

© 1995 by INPUT. Reproduction Prohibited.

The distribution of responses places 28% in both satisfactory and very satisfactory, respectively, and the addition of outstanding performance bring the total of all satisfactory or better ratings to 66%. Agency respondents rated the performance criteria somewhat satisfactory 19% of the time and definitely not satisfactory drew 15% of the responses.

H
Impacts and Trends

As agencies replace conventional paper documents with standardized computer forms, the use of electronic messaging, networked computers and information systems for conducting transactions is replacing activities formerly completed on paper or by telephone. Electronic commerce (EC) initiatives are working their way into the federal market at an accelerating pace and policy initiatives are attempting to keep up. Issues of authenticity and non-repudiation for electronic transactions, as well as privacy, integrity and time-stamping, are being addressed by policy makers as EC technologies evolve.

1. Security Policy Impact on Electronic Commerce

The impact of computer security policies and regulations on EC initiatives was examined, with results displayed in Exhibit IV-17. PKE techniques supporting digital signatures ranked highest, with EIE, popularly known as E-mail, the second-rated initiative in terms of policy impact.

Exhibit IV-17

Security Policy Impact on Electronic Commerce

Initiative	1	2	3	4	5
PKE (Digital Signature)	10	3	1	1	1
EFT	8	3	1	1	3
EIE (E-mail)	7	6	4	0	1
EDI	7	4	3	1	2

Total responses = 24 *Source: INPUT*

EDI and EFT both ranked lower at federal agencies but still scored well, reflecting both their importance in the commercial world and their advocacy in the NII initiative. The distribution of responses highlights agency interest in these initiatives. Nearly half of agency respondents, 48%, chose major impact on EC initiatives, followed by 24% some impact and 14% minimal impact. Only 5% said no impact and 11% chose don't know.

© 1995 by INPUT. Reproduction Prohibited.

2. Effects of Technology on Security Requirements

The questionnaire addressed the effects of technological change on agency computer security requirements. Many factors were identified and those drawing multiple responses are detailed in Exhibit IV-18. Agency respondents listed their technology concerns and the impact they expected through FY 1996. As multiple responses indicate, concern is high for security issues raised by Internet access, the growth of client/server computing, and the spread of open systems architecture. Software and encryption issues were highlighted as well.

Exhibit IV-18

Factors of Technological Change

Technology	Impact	Number of Responses
Internet Connectivity	High; new; impact across all bureaus; major impact from security standpoint; major; significant	5
Client/Server	Major impact from security standpoint; need for access controls, authentication and audit capabilities	4
PKE	Significant; major	4
EIE	Major; records storage	3
MISSI/Fortezza Cards	Major; providing security for DoD E-mail	3
Open Systems	High; greater demand for systems to address	3
Electronic Commerce	Major	2
Encryption	Significant; must implement through FY96	2
Increased Networking/ Multilevel Operations	Confidentiality, integrity and availability issues are surfacing	2
Software Issues	Move from DOS to Windows NT impacts hardware and software	2
WAN/LAN Installation	Greater need for access controls, authentication and audit capabilities	2

Total responses = 24 *Source: INPUT*

On the positive side, agencies view future technologies as delivering advances in security solutions to better meet the need for new products, such as improved encryption methods, more secure Internet access and advances in electronic commerce. One respondent noted that the requirements must be as dynamic as the technology.

© 1995 by INPUT. Reproduction Prohibited.

3. Impact of Non-Technical Market Factors

Agency respondents were asked to identify industry trends and non-technical business factors that could impact agency security plans. Exhibit IV-19 summarizes agency responses, with generally restrained views of any impact reflected.

Exhibit IV-19

Impact of Non-Technical Market Factors

Factor	1	2	3	4	5
Mergers	0	0	3	13	3
Acquisitions/Takeovers	0	0	3	13	3
Downsizing/Rightsizing	2	2	3	10	2
Business Process Reengineering	3	1	3	8	4
Shift in Business Focus	3	0	0	0	1
Stronger Industry Base*	1	0	0	0	0
Other Trends	1	0	1	0	0

** Greater capabilities as a result of this trend; security has benefited.*

Total responses = 24 *Source: INPUT*

A stronger industry base, producing greater capabilities with consequent benefits for security, was the only factor rated for major impact. A shift in business focus scored well, while other factors drew fewer responses. The distribution of responses points out the perception of non-technical business trends as having little impact on federal agency plans for computer security, and may indicate a lack of interest in this area.

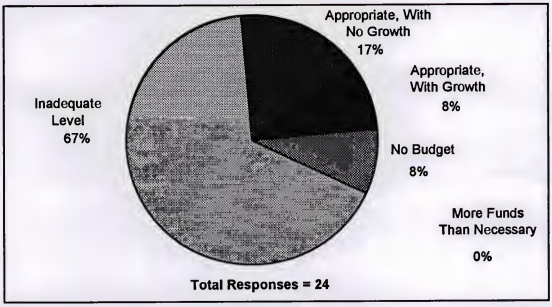
4. Impact of Budget Levels

The majority of agencies surveyed rated the impact of federal budgetary levels on implementation of their security plans. The variety of impacts, shown in Exhibit IV-20, reflects agency concerns with budgetary constraints. Additionally, respondents commented of the effects of shrinking budgets in forthright terms.

© 1995 by INPUT. Reproduction Prohibited.

Exhibit IV-20

Impact of Budgetary Levels



Source: INPUT

No respondents selected more funds than necessary and the next two levels, appropriate funding with and without growth accommodated, respectively, totaled only 25% of responses. Fully two-thirds of agency representatives cited inadequate funding to meet security needs.

The significant negative effect of budgetary constraints was evident in virtually all comments made. Respondents' comments on funding ranged from "getting worse" and "next to nothing" on to "budget so tight security is squeezed out." Agency representatives "are expected to do more with less; we have reached the point where things aren't getting done." One detailed comment addressed a potentially serious flaw in the design and development of security programs, a shortcoming that may hinder or delay the implementation of computer security plans. Agencies "need to dispel the myth that security is an overhead/administrative cost and therefore optional, and work to make it an integral part of system development costs. Programs are not accepting responsibility for appropriately budgeting for security costs. It often becomes the last item to be considered."

Some agencies have suffered major delays or cutbacks in acquisitions, and other agencies have downsized their levels of support and delayed implementation efforts. According to NIST, budgetary constraints have a significant impact on agencies' ability and willingness to implement computer security plans. Agencies have difficulty budgeting for security needs. There is no category in agencies' mandatory budget submission for computer security. They are supposed to include these costs in the overall

© 1995 by INPUT. Reproduction Prohibited.

system management category. Agencies find it difficult to reallocate funds for computer security. Also, computer security has to fight for new resources during the budgeting process. Traditional programs seem to receive continual funding while computer security must fight with new programs to receive funding. Finally, there is no national security requirement for non-DoD systems, making agencies less willing to spend funds on security they may view as nonessential.

5. Impact of Government Policies and Regulations

Computer security for federal information systems is subject to a range of governmental policies, regulations and other influences from policy formulating government entities. Accordingly, respondents from selected agencies were surveyed to obtain their view of the impact of various policies and regulations on their agency's computer security requirements and future acquisitions. Shown in Exhibit IV-21 are the agencies studied, and the range of responses listing impacts from major to insignificant.

Exhibit IV-21

Impact of Government Policies and Regulations

Factor	1	2	3	4	5
NIST	4	3	8	2	3
DoD/NSA	9	3	5	3	2
OMB	8	10	3	0	1
Other Policy Initiatives	1	8	2	2	0

Total responses = 24 *Source: INPUT*

In general, respondents viewed the activities and guidelines provided by OMB as beneficial. DoD/NSA were noted for development guidelines and for evaluation and certification of security products. NIST, despite the importance of its role and responsibilities, including standards setting under the Computer Security Act, received less recognition in the survey response than agencies with more proscribed roles. GSA was viewed as having minimal impact on the federal computer security market.

© 1995 by INPUT. Reproduction Prohibited.

(Blank)

© 1995 by INPUT. Reproduction Prohibited.

Competitive Trends

This section presents the results of INPUT's current vendor survey and other competitive information.

Vendors who responded to this survey provide a range of products and services to the federal computer security market and generate differing levels of revenue. They range in size from a 15-member, four-year-old entrepreneurial developer of high-technology security and privacy products to a telecommunications company with 250,000 employees.

Although the vendors favored defense agencies for information security sales opportunities, the DOJ ranked highest in number of agency opportunities, displacing the Treasury Department from that position. This finding suggests that many vendors recognize the special security concerns at DOJ and intend to participate in DOJ business.

Vendor respondents expect their computer security revenues to increase. The market is better defined in their view than in that of agency respondents. However, vendors do express a need for fewer real standards, as opposed to a multiplicity of overlapping and conflicting standards that not everyone uses.

A
Vendor Participation

1. Vendor Products and Services

Vendors were asked to identify the security products and services, categorized by market segment, that they sold to federal agencies. Of the three submodes of professional services, discussed in Section B of Chapter II, education and training rank highest with federal agencies and continue as important market components for vendors. Agencies indicated both near-term and longer interest in acquiring security awareness and training services. Exhibit V-1 shows the vendor products

© 1995 by INPUT. Reproduction Prohibited.

and services being provided now, and planned to be provided by the end of five years.

Exhibit V-1

Types of Security Products and Services Provided

	Current	2000
Hardware	4	3
Software	5	4
Integrated Solutions	4	5
Professional Services	5	5

Total responses - 8 *Source: INPUT*

The other professional services, both consulting and software development, comprise the balance of this market segment that rated highest among vendor respondents. Hardware accumulated only 20% of total responses while software and integrated services each drew 26%. However, the latter showed the only increase among the three in the next five years, supporting a trend to greater use of embedded security solutions derived from hardware/software integration, particularly those incorporating encryption technology.

Some of the vendors interviewed are new entrants to the federal computer security market and their responses concerned products under development. The majority of industry respondents also noted that they plan to provide additional security products and services in the future in response to demand from federal government clients.

B
Vendor Market Perceptions

Nearly three-fourths of the vendors surveyed viewed the federal computer security market as robust and identified a range of key factors contributing to the growth of this market. Market opportunities for information systems security reported by respondents are often the product of emerging technologies, dual-use applications migrating from the commercial sector, and the industry's response to evolving standards, regulations and guidelines driven by the first two factors.

1. State of the Federal Computer Security Market

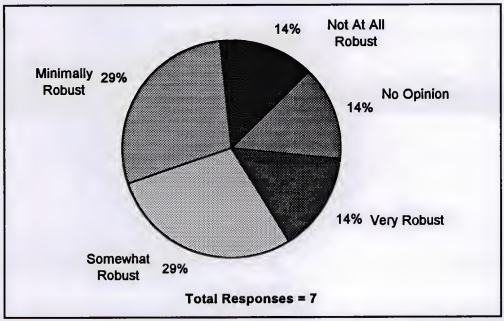
Most vendor respondents surveyed expected their firm's revenues from the federal computer security market to increase over the next five years. Vendors anticipated increases in their market share, from their ability to adapt both emerging and commercial technologies to federal market

© 1995 by INPUT. Reproduction Prohibited.

applications and from increased marketing efforts. Exhibit V-2 charts the state of the federal computer security market on a scale from very robust through not at all robust in four stages, and ending with no opinion.

Exhibit V-2

State of the Federal Computer Security Market



Source: INPUT

Seventy-two percent of respondents noted some degree of robustness in this market, while only 14% reported it without growth potential. The health of the market for security products and services was rated generally higher by the smaller vendors in INPUT's survey.

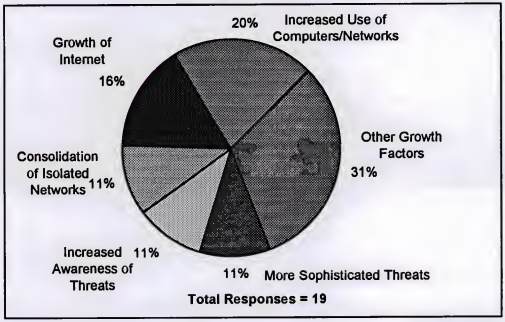
2. Growth Factors in the Federal Computer Security Market

Vendors anticipate growth in the market for automated information systems security as a result of numerous factors. Most prominent among them is the increased use of networks, underscoring a trend found in agency responses and noted in INPUT's past survey. The second and third place factors shown in Exhibit V-3, growth of Internet access and consolidation of classified networks, respectively, are closely related to the first in both technology and applicable security solutions.

© 1995 by INPUT. Reproduction Prohibited.

Exhibit V-3

Growth Factors in the Security Market



Source: INPUT

The proliferation of client/server computing and open systems architecture, in addition to the increasing use of networks from LANs and WANs to vast virtual private networks (VPNs), is driving the market for the security of the information itself, be it databases, files or even objects. Encryption technologies, on software platforms and embedded in firmware and hardware, are viewed as leading this market as standards and architectures evolve.

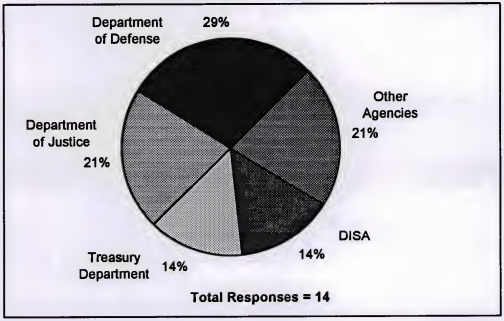
3. Leading Opportunities

The majority of vendors responding to INPUT's survey provide their products and services to both the civilian agencies and DoD. The INPUT questionnaire asked which agencies provide the most attractive opportunities for the sale of information security products and services. As shown in Exhibit V-4, the major defense agencies, DOJ and the Treasury Department were cited most frequently.

© 1995 by INPUT. Reproduction Prohibited.

Exhibit V-4

Federal Agency Opportunities



Source: INPUT

Among those agencies ranked by frequency of response, DISA was noted by 14% of respondents for driving both requirements and architectures for security. Additional agencies cited include NSA, as regulator and acknowledged expert on information security, Advanced Research Projects Agency (ARPA), for funding new and innovative developments for information security, and the CIA, for a strong need for security and privacy accompanied by a willingness to innovate. An overarching classification emerged from the survey, any agency connecting to the Internet, thereby expanding the market for firewalls in routers, bridges, gateways and servers, and secure E-mail protected by encryption technology.

4. Market Differences

Industry respondents' opinions on the differences between the civilian agency and defense markets is drawn from the past INPUT survey. A majority of respondents stated that more numerous and stricter requirements and standards are imposed upon the defense agencies than upon the civilian agencies. A second significant difference is the higher levels of both security awareness and experience among staff at defense agencies. While underway at many agencies, training to bring staff up to the required levels of awareness still is needed and presents a continuing opportunity for professional services firms.

© 1995 by INPUT. Reproduction Prohibited.

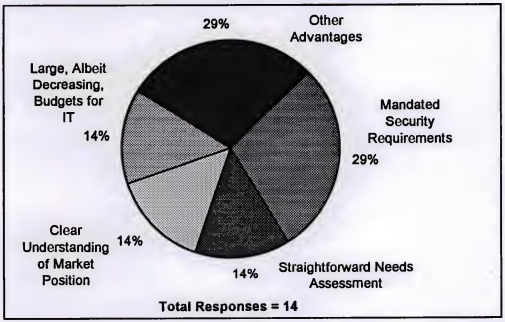
Defense agency missions, by their nature having greater volumes of classified information and higher levels of security, create increased potential for customized hardware, software and integrated security solutions. However, security of communications and networks has become critically important in some civilian agency programs, particularly at DOJ and the Treasury Department.

5. Competitive Advantages of the Federal Computer Security Market

In asking vendors to name the top three advantages of competing in the federal computer security market, INPUT received a wide range of opinions, summarized in Exhibit V-5. Mandated security requirements, the most mentioned advantage, provide distinct opportunities for security vendors.

Exhibit V-5

Competitive Advantages of the Federal Market



Source: INPUT

The closely related second place factor, straightforward needs assessment, derives from the established requirements and standards with which agencies and vendors must comply. A clear understanding of market position, receiving the same level of response, enables vendors to respond more directly to agency security needs.

Other advantages stated by vendor respondents include cost-driven migration to EDI, understanding of technology by a very educated customer base, and the increasing vulnerability of networks. The final

© 1995 by INPUT. Reproduction Prohibited.

factors, fewer competitors and a large, easily identified and focused market, combine for a clear advantage.

C
Vendor Performance

1. Ratings of Vendor Performance

Both agency and vendor respondents were asked to evaluate agency perceptions of vendor performance characteristics. Agency responses were taken from the current INPUT survey and largely paralleled those of the past survey with one exception. Encryption experience went from the highest rating, 3.3, to the lowest. The agency responses were in a moderate and much narrower range, 3.3 to 3.1, on the earlier survey. The vendor ratings of performance characteristics were determined in the past INPUT survey. Exhibit V-6 compares both vendors' and agencies' ratings of these characteristics.

Exhibit V-6

Comparative Ratings of Vendor Performance

Characteristic	Agency Rating	Vendor Rating
Successful Implementation	3.4	3.3
Support Experience	3.3	3.0
Staff Experience	3.2	3.1
Delivery Schedule	3.2	2.7
Training Experience	3.1	3.1
Hardware Offered	3.1	3.5
Software Offered	2.9	3.0
Price	2.8	3.0
Encryption Experience	2.5	3.4

Total responses: Agency = 24, Vendors = 8 *Source: INPUT*

Some differences of opinion appear between the two respondent groups. The characteristic rated most satisfactory by the vendors was hardware offered, whereas the agencies experienced somewhat lower levels of satisfaction for the products acquired. There are minor differences between the responses from the agencies and the vendors on most other characteristics. However, for their adherence to delivery schedules, the industry respondents rated performance at only 2.7, while agencies averaged a 3.2 rating for this characteristic. This suggests that vendors are already aware of their need to improve timely availability of products to levels consistent with agency perceptions of successful vendors.

© 1995 by INPUT. Reproduction Prohibited.

2. Suggested Improvements to Products and Services

Industry respondents were asked "what do you believe vendors need to do over the next five years to make their security products and services more valuable to the federal government?" The replies were as varied as the different types and levels of experience gained from the federal computer security market. Exhibit V-7 lists the responses, which continue a theme of customer orientation and user friendliness that was noted in INPUT's past survey.

Exhibit V-7

Suggested Improvements for Security Products and Services

Suggestion	Percent of Respondents*
Make Security Robust but Transparent	43
Listen Directly to End-users, Not Regulators, Prior to Building Products	43
Work to Achieve Generally Accepted Security Principles	29
Produce Functional Products At Reasonable Cost	29
Other	29
Build Products that Leverage Off Existing COTS Equipment	14

**Totals more than 100 due to multiple responses* *Source: INPUT*
Total responses = 8

Survey respondents cited the need to improve security solutions with respect to ease of use, pointing out that end-users need security but do not want the inconvenience that may be associated with use. Keeping solutions transparent to the user is a continuing objective, as is making security products friendly to unsophisticated users.

As noted in past INPUT federal market studies, the agencies again suggested improvements to implementation. This shows that implementation of security products, along with other areas of software and hardware, still remains an issue with many agency respondents. Perhaps another suggestion made by respondents—to stress security at the system development phase—would eliminate some implementation problems. In addition, early incorporation of security features would avoid the costs and inefficiencies associated with retrofitting systems with security measures at a later stage. The solution lies both with the agencies in stating requirements and with the vendors in providing for these measures.

In the past survey, vendors suggested standardizing security on off-the-shelf technology. A shift in emphasis, to the development of products based on COTS equipment, emerged in the current survey, underscoring

© 1995 by INPUT. Reproduction Prohibited.

the move to proven commercial solutions created in response to market demand.

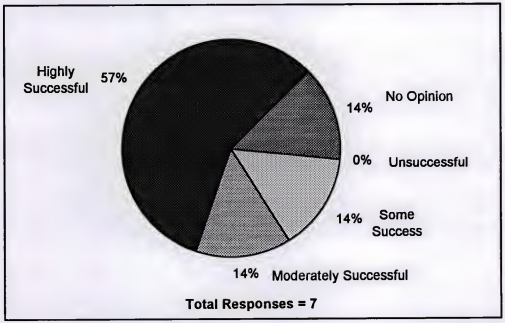
D
Teaming Patterns

1. Success of Teaming Efforts

Teaming efforts in the federal computer security market are becoming more frequent in order to respond adequately to the terms and conditions of many agency RFPs. A large majority of vendors view their teaming relationships as successful, with more than half choosing highly successful. Exhibit V-8 lists the respondents' rating of their level of success, which has improved significantly from the past INPUT survey.

Exhibit V-8

Success of Teaming Efforts



Source: INPUT

Those responding to the highest rating increased from 20% to 58%, while the responses for moderate and some success, respectively, declined to the 14% level. As before, none of the respondents found teaming efforts unsuccessful, and the vendors with no opinion declined as well.

2. Preferred Teaming Partners

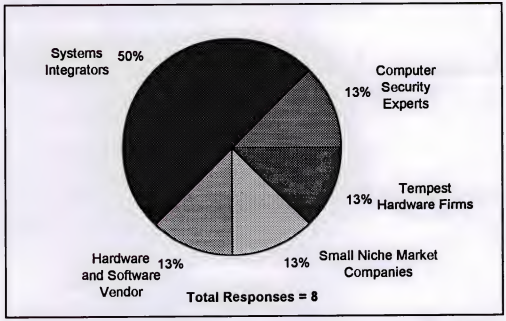
When asked to identify their most frequent or preferred type of teaming partner, industry respondents cited systems integrators most frequently. In a significant shift from the results of the past INPUT survey, this

© 1995 by INPUT. Reproduction Prohibited.

category has more than doubled the percentage of respondents naming systems integrators as the teaming partner of choice. Systems integrators are preferred for their ability to provide the requisite skills and resources for many federal programs and their understanding of the complexities of existing systems.

Exhibit V-9

Most Preferred Teaming Partner



Source: INPUT

As noted earlier, a number of the companies surveyed already are performing systems integration functions, or will be in the future. Hardware and software vendors combined declined to half the percentage of responses in the past survey. Also, in the next few years, teaming with small niche market companies may continue to increase as security requirements to be implemented call upon the specialized expertise of these companies.

Teaming activities present their own set of related vendor concerns and issues. As one respondent noted, it is easy to team, but hard to pick winners up front. Vendors recognize the need for communication and cooperation with teaming partners. Respondents also noted their own shortcomings in not fully identifying all program requirements early enough in the planning process. Industry representatives also have mentioned the need to improve marketing of their team members' products as well as increasing their reliance on COTS products. In addition, teaming efforts should focus on improving delivery schedules and product prices.

© 1995 by INPUT. Reproduction Prohibited.

E
Trends

1. Technology Trends

Vendor respondents noted that additional and more complex networking capabilities will increase automated information system access control requirements and will require development of encryption and other security safeguards for information storage and transmission. Expanded networks and increased Internet access are key technological factors affecting the federal computer security market over the next few years.

The increased use of PCs and workstations for end-user computing has driven the need for secure technology down to the level of the desktop at federal agencies. MLS systems, CMW and encryption capabilities down to the object level clearly show the efforts of security vendors to move into this segment of the federal computer security marketplace.

Standardization efforts continue to play a major role in the federal computer security market, with vendors working jointly with agencies and regulators on developing standards that incorporate commercial developments and private industry computer security expertise. Internetworking, new standards for interoperability and the implementation of open architectures all will contribute to the requirement for new levels of security.

Telecommunications developments such as photonics, supplanting opto-electronics, ATM and Synchronous Optical Network (SONET), and multimedia are technologies noted by respondents as shaping the future of federal computer security requirements and implementation. Vendors acknowledged that federal agencies need to go beyond just physical and software security solutions, that application portability security is needed, and that securing the information and not just the channel is a requirement of a secure environment in the future.

2. Budgetary Constraints

Vendors view delays in implementation, funding cuts and downsizing of security efforts as the main effects of federal budget constraints. Some viewed the effects as minimal because of decreasing product prices and increased purchase of commercial solutions below threshold exemptions from more costly procurement vehicles. However, many industry products still are considered costly by government agencies. As indicated in Chapter III, INPUT disagrees with this latter assessment and considers budget constraints to be the dominant negative market factor.

© 1995 by INPUT. Reproduction Prohibited.

Budget cuts will hinder the security training and implementation phases at many agencies, thus impacting market demand for some products and services negatively. Furthermore, cancellation or reduced funding for major programs can result in a lengthy procurement process and potential loss of acquisitions for the security component of the proposed system.

3. Market Trends

The marketplace is expected to change over the next two to five years as an influx of security solutions occurs. A growing family of Fortezza and Fortezza Plus products, CMW and MLS products and integrated encryption systems will be competing for market share with existing products.

Federal regulations, the Computer Security Act and the revised Appendix III of OMB Circular A-130 will provide guidance and direction to the industry. The NII initiative, the NPR and the escrowed encryption standard (EES) will give additional weight to the importance of security for federal information systems and may spark greater demand for products and services.

Automated information systems security, in its most current interpretation, is a component of IT. The future market is IT with integrated security features. Emerging trends in the federal computer security market are the increasing use of security as a discriminator by users, and the eventual availability of security for free as the IT market evolves.

© 1995 by INPUT. Reproduction Prohibited.

Federal Agency Respondent Profile

Interviews in 1995 were conducted by telephone, facsimile and mail. The respondents interviewed included administrative policy officials, contracting officers, and program managers in the following agencies:

Department of Commerce

- Office of the Secretary
- NTIA

Department of Defense

- C3I Security
- ARPA
- DISA
- DLA
- Department of the Air Force
- Department of the Army
- Department of the Navy
- Marine Corps

Department of Education

Department of Health and Human Services

Department of the Interior

© 1995 by INPUT. Reproduction Prohibited.

Department of Justice

- Justice Management Division
- Drug Enforcement Administration
- Immigration and Naturalization Service

Department of Labor

NASA

United States Postal Service

Department of State

Department of Transportation

- Office of the Secretary
- Federal Aviation Administration
- United States Coast Guard

Department of the Treasury

- United States Customs Service.

A
Vendor Respondent Profile

Interviews in 1995 were conducted by telephone, facsimile and mail. INPUT contacted a representative sample of contractors that provided or planned to provide computer security products and services to the federal government.

Job classifications among individual vendor respondents included marketing personnel, program managers, and administrative executives.

Interviews with vendor personnel were conducted by telephone, facsimile and in person at the following companies:

AT&T

Digital Equipment Corporation

General Kinetics, Inc.

© 1995 by INPUT. Reproduction Prohibited.

Harris Computer Systems Corporation

SAIC

Secure Computing Corporation

TECSEC, Incorporated

Trusted Information Systems, Inc.

© 1995 by INPUT. Reproduction Prohibited.

(Blank)

© 1995 by INPUT. Reproduction Prohibited.

B

Glossary of Federal Acronyms

Acronyms and contract terms that INPUT encountered most often in program documentation and interviews for this report are included here, but this glossary should not be considered all-inclusive. Federal procurement regulations (DAR, FPR, FAR, FIRMR, FPMR) and contract terms listed in RFIs, RFPs, and RFQs provide applicable terms and definitions.

Federal agency acronyms have been included to the extent they are employed in this report.

A
Federal Acronyms

AAS	Automatic Addressing System
ACTS	Advanced Communications Technology Satellite
ADNET	Anti-Drug Network
ADS	Automatic Digital Switches (DCS)
AMPE	Automated Message Processing Equipment
AMPS	Automated Message Processing System
ARPA	Advanced Research Projects Agency
ASP	Aggregated Switch Procurement
AUTODIN	AUTOmatic DIgital Network of the Defense Communications System
AUTOSEVOCOM	AUTOmatic SEcure VOice COMmunications Network

© 1995 by INPUT. Reproduction Prohibited.

AUTOVON	AUTOmatic VOice Network of the Defense Communications System
Benchmark	Method of evaluating ability of a candidate computer system to meet user requirements
C4	Command, Control, Communications, and Computers
C3I	Command, Control, Communications, and Intelligence
CCEP	Commercial Comsec Endorsement Program
CISS	Center for Information Systems Security
COMSTAT	Communications Satellite Corporation
CSL	Computer Systems Laboratory (NIST)
CSSPAB	Computer Systems Security and Privacy Advisory Board (NIST)
DCS	Defense Communications System
DCTN	Defense Commercial Telecommunications Network
DDL	Digital Data Link
DDN	Defense Data Network
DES	Data Encryption Standard
DES MAC	Data Encryption Standard Massage Authentication Control
DMS	Defense Message System
DOJ	Department of Justice
DSCS	Defense Satellite Communication System
DSN	Defense Switched Network
DSP	Defense Support Program (WWMCCS)
DTN	Defense Transmission Network
FCC	Federal Communications Commission
FEDCAC	Federal Computer Acquisition Center (GSA)

© 1995 by INPUT. Reproduction Prohibited.

FEDSIM	Federal Systems Integration and Managment Center (GSA)
FIPS	NIST Federal Information Processing Standard
FIRMR	Federal Information Resource Management Regulations
FISSP	Federal Information Systems Support Program (GSA)
FSTS	Federal Secure Telecommunications System
FTSP	Federal Telecommunications Standards Program administered by NCS; Standards are published by GSA
FTS	Federal Telecommunications System
FTS2000	Replacement of the Federal Telecommunications System
GAO	General Accounting Office
GSSPs	Generally Accepted System Security Principles
HHS	Health and Human Services
IRS	Internal Revenue Service
KEA	Key Exchange Algorithm - classified encryption algorithm
MLS	Multilevel Security
MYK78	Clipper chip
MYK80	Capstone chip
NCSC	National Computer Security Center (NSA)
NII	National Information Infrastructure
NIST	National Institute of Standards and Technology
NISTR	NIST Internal Report
NPR	National Performance Review
NSA	National Security Agency
NSEP	National Security and Emergency Preparedness.
NSIA	National Security Industrial Association

© 1995 by INPUT. Reproduction Prohibited.

NSTAC	National Security Telecommunications Advisory Council
NSTISSC	National Security Telecommunications and Information Systems Security Committee
POTS	Purchase of Telephone Systems
SDN	Secure Data Network
STU	Secure Telephone Unit
TCP/IP	Transmission Control Protocol/Internet Protocol
TCSEC	Trusted Computer Security Evaluation Criteria (Orange Book)
TEMPEST	Studies, inspections, and tests of unintentional electromagnetic radiation from computer, communication, command, and control equipment that may cause unauthorized disclosure of information; usually applied to DoD and security agency testing programs
TTAP	Trusted Technology Assessment Program (NIST)
VICI	Voice Input Code Identifier
WWMCCS	World Wide Military Command and Control System

B
General and Industry Acronyms

ADAPSO	Association of Data Processing Service Organization, now the Computer Software and Services Industry Association (See ITAA)
ADPE	Automated Data Processing Equipment
ANSI	American National Standards Institute
ATM	Asynchronous Transmission Mode
CCIA	Computers and Communications Industry Association
CCITT	Comité Consultatif Internationale de Télégraphique et Téléphonique (Commttee of the International Telecommunication Union); (See ITU-T)
COS	Corporation for Open Systems

© 1995 by INPUT. Reproduction Prohibited.

COTS	Commercial Off-The-Shelf
EC	Electronic Commerce
EDI	Electronic Data Interchange
ETSI	European Telecommunications Standards Institute
ISDN	Integrated Services Digital Networks
ISSA	Information Systems Security Association
ISO	International Organization for Standardization; voluntary international standards organization and member of CCITT
ITU	International Telecommunication Union
LAN	Local Area Network
PCMCIA	Personal Computer Memory Card International Association
RBOC	Regional Bell Operating Company
RSA	Rural Service Area
SONET	Synchronous Optical Network
VPN	Virtual Private Network
WAN	Wide Area Network

© 1995 by INPUT. Reproduction Prohibited.

(Blank)

© 1995 by INPUT. Reproduction Prohibited.

C

Policies, Regulations and Standards

A
OMB Circulars and Bulletins

Circular A-130	Management of Federal Information Resources
Bulletin 88-16	Guidance for Preparation and Submission of Security Plans for Federal Computer Systems Containing Sensitive Information
Bulletin 90-08	Guidance for Preparation of Security Plans for Federal Computer Systems That Contain Sensitive Information

B
DoD Directives

DD-5200.28	Security Requirements for Automatic Data Processing (ADP) Systems
DD-5200.28-M	Manual of Techniques and Procedures for Implementing, Deactivating, Testing, and Evaluating Secure Resource Sharing ADP Systems

C
Standards

FIPS PUB 31	Guidelines for ADP Physical Security and Risk Management
FIPS PUB 39	Glossary for Computer Systems Security

© 1995 by INPUT. Reproduction Prohibited.

FIPS PUB 41	Computer Security Guidelines for Implementing the Privacy Act of 1974
FIPS PUB 46	Data Encryption Standard (DES)
FIPS PUB 46-1	Data Encryption Standard (Reaffirmed until 1993)
FIPS PUB 46-2	Data Encryption Standard (Reaffirmed until 1998)
FIPS PUB 65	Guidelines for Automatic Data Processing Risk Analysis
FIPS PUB 73	Guidelines for Security of Computer Applications
FIPS PUB 74	Guidelines for Implementing and Using the NBS Data Encryption Standard
FIPS PUB 102	Guidelines for Computer Security Certification and Accreditation
FIPS PUB 112	Standard on Password Usage
FIPS PUB 139	Interoperability and Security Requirements for Use of the Data Encryption Standard in the Physical Layer of Data Communications
FIPS PUB 140	General Security Requirements for Equipment Using the Data Encryption Standard
FIPS PUB 141	Interoperability and Security Requirements for Use of the Data Encryption Standard with CCITT Group 3 Facsimile Equipment
FIPS PUB 185	Escrowed Encryption Standard
FIPS PUB 186	Digital Signature Standard

© 1995 by INPUT. Reproduction Prohibited.

D

OMB Circular A-130 Appendix III

The Office of Management and Budget (OMB) has proposed the revision of Appendix III of Circular No. A-130, Security of Federal Automated Information Systems. Publication of the revision, with the incorporation of comments from interested parties, is projected for the beginning of Fiscal Year 1996.

For further information, contact Ed Springer, Information Policy and Technology Branch, Office of Information and Regulatory Affairs, Office of Management and Budget, Room 10236, New Executive Office Building, Washington, D.C. 20503. Telephone: (202) 395-3785.

Appendix III

TO OMB CIRCULAR NO. A-130

SECURITY OF FEDERAL AUTOMATED INFORMATION

1. Purpose

This Appendix establishes a minimum set of controls to be included in Federal automated information security programs; assigns Federal agency responsibilities for the security of automated information; and links agency automated information security programs and agency management control systems established in accordance with OMB Circular No. A-123. The Appendix revises procedures formerly contained in Appendix III to OMB Circular No. A-130 (50 FR 52730; December 24, 1985), and incorporates requirements of the Computer Security Act of 1987 (P.L. 100-235) and responsibilities assigned in applicable national security directives.

© 1995 by INPUT. Reproduction Prohibited.

2. Definitions

The term:

a. "adequate security" means security commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information. This includes assuring that systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, personnel, operational, and technical controls.

b. "application" means the use of information resources (information and information technology) to satisfy a specific set of user requirements.

c. "general support system" or "system" means an interconnected set of information resources under the same direct management control which share common functionality. A system normally includes hardware, software, information, data, applications, and people. A system can be, for example, a local area network (LAN) including smart terminals that supports a branch office, an agency-wide backbone, a communications network, a departmental data processing center including its operating system and utilities, a tactical radio network, or a shared information processing service organization (IPSO).

d. "major application" means an application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Note: All Federal information requires some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as major. Adequate security for other applications should be provided by security of the systems in which they operate.

3. Automated Information Security Programs. Agencies should implement and maintain a program to assure that adequate security is provided for all agency information collected, processed, transmitted, stored, or disseminated in general support systems and major applications.

Each agency's program should implement policies, standards and procedures which are consistent with government-wide policies, standards, and procedures issued by the Office of Management and Budget, the Department of Commerce, the General Services Administration and the Office of Personnel Management (OPM). Different or more stringent requirements for securing national security information should be incorporated into agency programs as required by

© 1995 by INPUT. Reproduction Prohibited.

appropriate national security directives. At a minimum, agency programs should include the following controls in their general support systems and major applications:

a. Controls for general support systems.

1) Assign Responsibility for Security. Assign responsibility for security in each system to an official knowledgeable in the information technology used in the system and in providing security for such technology.

2) System Security Plan. Plan for the security of each general support system as part of the organization's information resources management (IRM) planning process. The security plan should be consistent with guidance issued by the National Institute of Standards and Technology (NIST). Independent advice and comment on the security plan should be solicited prior to the plan's implementation. A summary of the security plans should be incorporated into the 5-year IRM plan required by the Paperwork Reduction Act (44 U.S.C. Chapter 35) and Section 8(b) of this circular. Security plans should include:

a) Rules of the System. Establish a set of rules of behavior concerning use of, security in, and the acceptable level of risk for the system. The rules should be based on the needs of the various users of the system. The security required by the rules should be only as stringent as necessary to provide adequate security for information in the system. Such rules should clearly delineate responsibilities and expected behavior of all individuals with access to the system. They should also include appropriate limits on interconnections to other systems and should define service provision and restoration priorities. Finally, they should be clear about the consequences of behavior not consistent with the rules.

b) Awareness and Training. Ensure that all individuals are aware of their security responsibilities and trained how to fulfill them before allowing them access to the system. Such awareness and training should assure that individuals are versed in the rules of the system, be consistent with guidance issued by NIST and OPM, and apprise individuals about available assistance and technical security products and techniques. Behavior consistent with the rules of the system and periodic refresher training should be required for continued access to the system.

c) Personnel Controls. Screen all individuals who are authorized to bypass technical and operational security controls of the system (e.g., LAN administrators or system programmers) commensurate with the risk and magnitude of loss or harm they could cause. Such screening should occur prior to the individuals' being authorized to bypass controls and periodically thereafter.

© 1995 by INPUT. Reproduction Prohibited.

d) Incident Response Capability. Ensure that there is a capability to provide help to users when a security incident occurs in the system and to share information concerning common vulnerabilities and threats. This capability should coordinate with those in other organizations and should assist the agency in pursuing appropriate legal action, consistent with Department of Justice guidance.

e) Continuity of Support. Establish and periodically test the capability to continue providing service within a system based upon the needs and priorities of the participants of the system.

f) Technical Security. Ensure that cost-effective security products and techniques are appropriately used within the system.

g) System Interconnection. Obtain written management authorization based upon the acceptance of risk to the system prior to connecting with other systems. Where connection is authorized, controls should be established which are consistent with the rules of the system and in accordance with guidance from NIST.

3) Review of Security Controls. Periodically review the security controls in each system commensurate with the acceptable level of risk for the system established in its rules, especially when significant modifications are made and at least every 3 years. Depending on the potential risk and magnitude of harm that could occur, consider identifying a deficiency pursuant to OMB Circular No. A-123, "Management Accountability and Control" and the Federal Managers' Financial Integrity Act (FMFIA), if there is no assignment of security responsibility, no security plan or no authorization to process in a system.

4) Authorize Processing. Ensure that a management official authorizes in writing the use of each general support system based on implementation of its security plan before beginning or significantly changing processing in the system. Use of the system should be re-authorized at least every three years.

b. Controls for Major Applications.

1) Assign Responsibility for Security. Assign responsibility for security of each major application to a management official knowledgeable in the nature of the information processed by the application and in the management, operational, and technical controls used to protect it. This official should assure that effective security products and techniques are appropriately used in the application and should be contacted when a security incident occurs concerning the application.

© 1995 by INPUT. Reproduction Prohibited.

2) Application Security Plan. Plan for the adequate security of each major application, taking into account the security of all systems in which the application will operate. The plan should be consistent with guidance issued by NIST. Advice and comment on the plan should be solicited from the official responsible for security in the primary system in which the application will operate prior to the plan's implementation. A summary of the security plans should be incorporated into the 5-year IRM plan required by the Paperwork Reduction Act. Application security plans should include:

a) Application Rules. Establish a set of rules concerning use of and behavior within the application. The rules should be as stringent as necessary to provide adequate security for the application and the information in it. Such rules should clearly delineate responsibilities and expected behavior of all individuals with access to the application. In addition, the rules should be clear about the consequences of behavior not consistent with the rules.

b) Specialized Awareness and Training. Before allowing individuals access to the application, ensure that all individuals receive specialized awareness and training focused on their responsibilities and the application rules. This may be in addition to the awareness and training required for access to a system. Such awareness and training may vary from a notification at the time of access (e.g., for members of the public using an information retrieval application) to formal training (e.g., for an employee that works with a high risk application).

c) Personnel Security. Incorporate controls such as separation of duties, least privilege and individual accountability into the application as appropriate. In cases where such controls cannot adequately protect the application and information in it, screen individuals commensurate with the risk and magnitude of the harm they could cause. Such screening should be done prior to the individuals being authorized to access the application and periodically thereafter.

d) Contingency Planning. Establish and periodically test the capability to perform the agency function supported by the application in the event of failure of its automated support.

e) Technical Controls. Ensure that appropriate security controls are specified, designed into, tested, and accepted in accordance with guidance issued by NIST.

f) Information Sharing. Ensure that information shared from the application is protected appropriately, relative to the protection provided when information is within the application.

© 1995 by INPUT. Reproduction Prohibited.

g) Public Access Controls. Where an agency's application promotes or permits public access, additional security controls should be added to protect the integrity of the application and the confidence the public has in the application. Such controls should include segregating information made directly accessible to the public from official agency records (e.g., by putting information onto a bulletin board).

3) Review of Application Controls. Perform an independent review or audit of the security controls in each application at least every three years. Consider identifying a deficiency pursuant to the Federal Managers' Financial Integrity Act if there is no assignment of responsibility for security, no security plan, or no authorization to process for the application.

4) Authorize Processing. Ensure that a management official authorizes in writing use of the application by confirming that its security plan as implemented adequately secures the application. Results of the most recent review or audit of controls should be a factor in management authorizations. The application should be authorized prior to operating and re-authorized at least every three years thereafter. Management authorization implies accepting the risk of each system used by the application.

4. Assignment of Responsibilities

a. Department of Commerce. The Secretary of Commerce should:

1) Develop and issue appropriate standards and guidance for the security of sensitive information in Federal computer systems.

2) Review and update guidelines for training in computer security awareness and accepted computer security practice, with assistance from OPM.

3) Provide agencies guidance for security planning to assist in their development of application and system security plans.

4) Provide guidance and assistance, as appropriate, to agencies concerning effective controls when interconnecting with other systems.

5) Coordinate agency incident response activities to promote sharing of incident response information and related vulnerabilities.

6) Evaluate new information technologies to assess their security vulnerabilities, with technical assistance from the Department of Defense, and apprise Federal agencies of such vulnerabilities as soon as they are known.

© 1995 by INPUT. Reproduction Prohibited.

b. Security Policy Board. The Security Policy Board should:

1) Act, in accordance with applicable national security directives, to coordinate the security activities of the Federal government regarding the security of automated information systems that process national security information;

c. Department of Defense. The Secretary of Defense should:

1) Provide appropriate technical advice and assistance (including work products) to the Department of Commerce.

2) Assist the Department of Commerce in evaluating the vulnerabilities of emerging information technologies.

d. Office of Personnel Management. The Director of the Office of Personnel Management should:

1) Assure that its regulations concerning computer security training for Federal civilian employees are effective.

2) Assist the Department of Commerce in updating and maintaining guidelines for training in computer security awareness and accepted computer security practice.

e. General Services Administration. The Administrator of General Services should:

1) Assure that the Federal Information Resources Management Regulation provides guidance to agencies on addressing security considerations when acquiring automated data processing equipment (as defined in section 111(a)(2) of the Federal Property and Administrative Services Act of 1949, as amended).

2) Facilitate the development of contract vehicles for agencies to use in the acquisition of cost-effective security products and services (e.g., back-up services contract).

3) Provide appropriate security services to meet the needs of Federal agencies to the extent that such services are cost-effective.

f. Department of Justice. The Attorney General should:

1) Provide guidance to agencies on legal remedies regarding security incidents and ways to report and work with law enforcement concerning such incidents.

2) Pursue appropriate legal actions when security incidents occur.

© 1995 by INPUT. Reproduction Prohibited.

5. Correction of Deficiencies and Reports

a. Correction of Deficiencies. Agencies shall correct deficiencies which are identified through the reviews of security for systems and major applications described above.

b. Reports on Deficiencies. In accordance with OMB Circular No. A-123, if a deficiency in controls is judged by the agency head to be material when weighed against other agency deficiencies, it should be included in the annual FMFIA report. Less significant deficiencies should be reported and progress on corrective actions tracked at the appropriate agency level.

c. Summaries of Security Plans. Agencies shall include a summary of their system security plans and major application plans in the five-year plan required by the Paperwork Reduction Act (44 U.S.C. 3505).

© 1995 by INPUT. Reproduction Prohibited.

Related INPUT Reports

A
Annual Market Sales

U.S. Information Services Cross-Industry Markets, 1995–2000

Procurement Analysis Reports

B
Market Reports

Federal Telecommunications Market, 1994–1999

Federal Information Systems and Services, 1994–1999

Federal High Performance Computing, 1994–1999

Federal E-Mail Systems Market

Client/Server Trends in the Federal IT Market, 1994

© 1995 by INPUT. Reproduction Prohibited.

(Blank)

© 1995 by INPUT. Reproduction Prohibited.

Questionnaires

A
Agency Questionnaire

Federal Computer Security Market

Section I - Security Plan

1. What do you believe is the purpose of the security plan implemented by your agency?

   - ☐ Improve awareness
   - ☐ Set policy for behavior
   - ☐ Identify solutions
   - ☐ Respond to requirements of law
   - ☐ Other _____

2. To what degree do you think your agency's implementation of a security plan is effective? Please rate on a scale of 1 to 5. 1 = Very effective, no weaknesses; 2 = Mostly effective, minor weaknesses; 3 = Marginally effective; 4 = Ineffective; and 5 = Not implemented at all.

   1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐

3. Does your agency periodically review security controls?

Upon significant system modification	Yes ☐	No ☐
Every three years	Yes ☐	No ☐

4. Is system use authorized in writing based on the security plan?

Before beginning or significantly changing processing	Yes ☐	No ☐
Every three years	Yes ☐	No ☐

© 1995 by INPUT. Reproduction Prohibited.

5. What directives and guidelines regarding computer security does your agency use in addition to OMB Circular A-130 Appendix III?

_____
_____
_____
_____

6. Has the shift from the measurement of risk to the management of risk (the emphasis of Appendix III of OMB Circular No. A-130) impacted your agency's computer security plans and operations? Please rate on a scale of 1 to 5. 1 = Major impact; 2 = Some impact; 3 = Minimal impact; 4 = No impact; and 5 = No shift.

1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐

7. Which of the following computer security products and services does your agency plan to acquire? Please check all that apply.

Administrative:	within 2 years	3-5 years
Contractor assistance for preparation of plans	☐	☐
Decentralized security administration	☐	☐
Regular security audits	☐	☐
Risk assessment/analysis	☐	☐
Security education	☐	☐
Other contractor support	☐	☐
Hardware:		
Backup power supply	☐	☐
Communications security products	☐	☐
On-line backup of files	☐	☐
Secure telephones	☐	☐
Secure workstations	☐	☐
Separate computer for software testing	☐	☐
Other contractor security devices	☐	☐
Physical security:		
Computer room security	☐	☐
Emission control devices	☐	☐
Offsite storage of backup files	☐	☐
Tempest products	☐	☐

© 1995 by INPUT. Reproduction Prohibited.

Software:	Within 2 years	3-5 years
Access control software	☐	☐
Antivirus software	☐	☐
Automatic file backup	☐	☐
Dial-up port protection	☐	☐
Encryption	☐	☐
Message authentication	☐	☐
Network access control	☐	☐
Password management	☐	☐
Secure UNIX-based products	☐	☐
Single sign-on	☐	☐
Other:		
Distributed system security architecture (DSSA)	☐	☐
ITSEC-certified products	☐	☐
NCSC-certified products	☐	☐

8. What does your security plan cover? Please check all that apply.

☐ Client/Server	☐ Computer ethics
☐ Disgruntled employees	☐ Document control
☐ Employee handbook	☐ Industrial espionage
☐ Information leaks	☐ Insufficient security
☐ Internet access	☐ Laptop
☐ Data center	☐ Micro
☐ Natural disasters	☐ Network access
☐ Network hackers	☐ Password control
☐ PBX fraud	☐ Proprietary information
☐ Software use	☐ System access
☐ Terrorism	☐ Theft of equipment
☐ Viruses & malicious code	☐ Other _____

Section II - Implementation

9. Has back-up and restoration of services capability been established?

Yes ☐ No ☐

© 1995 by INPUT. Reproduction Prohibited.

10. Do you believe there are cost-effective solutions to your security requirements? Yes ☐ No ☐

11. Is authorized interconnection with other systems subject to consistent security controls? Yes ☐ No ☐

12. Is security developed for major applications extended to information shared outside the system? Yes ☐ No ☐

13. Is public access subject to security controls on the following?

Computer systems	Yes ☐	No ☐
Major applications	Yes ☐	No ☐
Bulletin boards	Yes ☐	No ☐

Section III - Performance of Products and Services

14. What priority has your agency assigned for the following performance criteria?

Criteria	High Priority	Low Priority	None
Access control	☐	☐	☐
Back-up and recovery provisions	☐	☐	☐
Continued service	☐	☐	☐
No security breaches	☐	☐	☐
Physical security	☐	☐	☐
Other _____	☐	☐	☐

15. How successful have industry products and services been in meeting the current criteria? Please rate on a scale of 1 to 5. 1 = Extremely well; 2 = Well; 3 = Some success; 4 = Limited success; and 5 = Not at all.

1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐

16. Have you used or do you intend to use a GSA contractor to support your security needs?

_____

17. If so, which contractor and in what way?

_____

_____

© 1995 by INPUT. Reproduction Prohibited.

18. On a scale of 1 to 5, with 1 being very important and 5 not important, please rate the following selection criteria for computer security products and services.

Criteria	1	2	3	4	5
Ease of implementation	☐	☐	☐	☐	☐
Encryption features	☐	☐	☐	☐	☐
Password systems	☐	☐	☐	☐	☐
Product/service price	☐	☐	☐	☐	☐
Secure network capabilities	☐	☐	☐	☐	☐
Training features	☐	☐	☐	☐	☐
Vendor's federal experience	☐	☐	☐	☐	☐
Vendor's support reputation	☐	☐	☐	☐	☐
Other _____	☐	☐	☐	☐	☐

19. Which methods of acquisition does your agency use for its purchase of computer security products and services? (*Please check all that apply and circle method most often used.*)

☐ GSA Schedules

☐ RFP for requirement contract

☐ RFPs for specific purchase

☐ Purchase as part of other procurements

☐ Other _____

20. What type of vendor or organization appears most appropriate for providing computer security products/services for your agency?

☐ Aerospace divisions ☐ Hardware vendors

☐ Not-for-profit firms ☐ Professional services firms

☐ Software vendors ☐ Systems integrators

☐ Other _____

21. Please rate the following computer security vendor characteristics with respect to performance for your agency on a scale of 1 to 5.
1 = Outstanding performance; 2 = Very satisfactory; 3 = Satisfactory; 4 = Somewhat satisfactory; and 5 = Definitely not satisfactory.

Criterion	1	2	3	4	5
Delivery schedule	☐	☐	☐	☐	☐
Encryption experience	☐	☐	☐	☐	☐

© 1995 by INPUT. Reproduction Prohibited.

	1	2	3	4	5
Hardware offered	☐	☐	☐	☐	☐
Price	☐	☐	☐	☐	☐
Software offered	☐	☐	☐	☐	☐
Staff experience	☐	☐	☐	☐	☐
Successful implementation	☐	☐	☐	☐	☐
Support experience	☐	☐	☐	☐	☐
Training experience	☐	☐	☐	☐	☐
Other _____	☐	☐	☐	☐	☐

Section IV - Impacts/Trends

22. Please rate, on a scale of 1 to 5, the impact of computer security policies and regulations on the following Electronic Commerce initiatives.
1 = Major impact; 2 = Some impact; 3 = Minimal impact; 4 = No impact; and 5 = Don't know.

Initiative	1	2	3	4	5
EDI	☐	☐	☐	☐	☐
EIE (E-mail)	☐	☐	☐	☐	☐
EFT	☐	☐	☐	☐	☐
PKE (digital signature)	☐	☐	☐	☐	☐

23. How are technological changes affecting your agency's computer security requirements through FY 1996?

Technology	Impact
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____

© 1995 by INPUT. Reproduction Prohibited.

24. What impact have industry or market factors (non-technical) had on your agency's computer security plans? Please rate on a scale of 1 to 5. 1 = Major impact; 2 = Some impact; 3 = Minimal impact; 4 = No impact; and 5 = Don't know.

Factor	1	2	3	4	5
Mergers	☐	☐	☐	☐	☐
Acquisitions/takeovers	☐	☐	☐	☐	☐
Downsizing/rightsizing	☐	☐	☐	☐	☐
Business process reingineering	☐	☐	☐	☐	☐
Other trends _____	☐	☐	☐	☐	☐

25. Please rate, on a scale of 1 to 5, the impact of federal budgetary levels on implementing your agency's computer security plans. 1 = More funds than necessary; 2 = Appropriate, with growth expected; 3 = Appropriate with no growth; 4 = Inadequate level; and 5 = No budget.

1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐

Comments _____

_____

26. On a scale of 1 to 5, with 1 being major and 5 insignificant, please rate the impact of government policies or regulations from each of the following on your agency's computer security requirements and acquisitions through FY 1996?

Agency	1	2	3	4	5
NIST	☐	☐	☐	☐	☐
DOD/NSA	☐	☐	☐	☐	☐
OMB	☐	☐	☐	☐	☐
Other legislative or regulatory policy initiatives	☐	☐	☐	☐	☐

Comments _____

_____

Thank you for your cooperation and assistance!

© 1995 by INPUT. Reproduction Prohibited.

B
Vendor Questionnaire

Federal Computer Security Market

1. From the following list, please identify the types of products or services you currently provide or plan to provide by 2000.

Product or Service	Current	2000
Hardware	☐	☐
Software	☐	☐
Integrated Solutions	☐	☐
Professional services	☐	☐

2. Please describe the state of the federal computer security market on a scale of 1 to 5. 1 = Very robust; 2 = Somewhat robust; 3 = Minimally robust; 4 = Not at all robust; and 5 = No opinion.

1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐

3. Please identify the top three key factors that will contribute to the growth of the federal security market.

_____

_____

4. In your opinion, which agencies provide the most attractive opportunities for information security products and services? Why?

_____

_____

5. What are the top three advantages of competing in the federal computer security market?

_____

_____

6. What do you believe vendors need to do over the next 5 years to make their security products and services more valuable to the federal government?

_____

_____

© 1995 by INPUT. Reproduction Prohibited.

7. Please rate your level of success with teaming efforts in the federal computer security market on a scale of 1 to 5. 1 = Highly successful; 2 = Moderately successful; 3 = Some success; 4 = Unsuccessful; and 5 = No opinion.

1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐

8. Please identify your firm's most frequent/preferred type of teaming partner.

Hardware and software vendors	☐
Hardware manufacturers and professional services firms	☐
Hardware manufacturers and systems integrators	☐
Small market niche companies	☐
Software firms	☐
System integrators	☐
Tempest hardware firms	☐
Other _____	☐

© 1995 by INPUT. Reproduction Prohibited.

(Blank)

© 1995 by INPUT. Reproduction Prohibited.

Computer Security Opportunities

The opportunities shown in the table below are not all-inclusive. The program and values specified here are for the overall system, including security. The percentage of the total that applies to security is not known at this time.

Computer Security Opportunities in the Federal Government

Department	Program	RFP Date	Value
Air Force	Base Level Systems Modernization II (BLSM II)	7/95	$100 Million
	Network Support Services (NSS)	8/95	Unknown
Army	Systems Engineering and Technical Assistance for ASAS	9/97	Unknown
Defense	Wireless Communications (Governmentwide)	1996	Unknown
	ADP Support for Defense Mapping Agency	7/95	Unknown
	Defense Research Engineering Network (DREN)	8/95	$1.4 Billion
	Joint Information Management Support (JIMS)	8/95	$10 Million
	Joint Interoperability Engineering Omnibus	12/95	$100 Million
	Defense Information Systems Network	1996	Unknown
Energy	ADP Support for Albuquerque	7/95	$40 Million
	Automated Procurement Express System (APES)	1/96	Unknown
GSA	Post-FTS2000 Contracts	1QFY96	$25 Billion
HHS	ADP Support for the PHS	6/97	$20 Million
	Data Transformation Software	10/95	Unknown
	Telecommunications Services for HRSA	11/95	Unknown
Justice	FBI-DEA Administrative Network	3/96	Unknown
	Justice Consolidated Network	1/96	Unknown
Transportation	Facilities Management for TCC	10/96	$40 Million
Treasury	Upgrade of Computer Security	7/95	Unknown

Source: INPUT

© 1995 by INPUT. Reproduction Prohibited.

(Blank)

© 1995 by INPUT. Reproduction Prohibited.

Security Vendors

A
Security Devices

AT&T Network Systems[1]
Blue Star Marketing, Inc.[1]
BTG, Inc.[1]
CIS Security Systems Corporation[1]
Dedicated Micros[1]
Digital Equipment Corporation[2]
FiberPlex Incorporated[1]
Greystone Peripherals, Inc.[1]
GRI Secure Communications[1]
Information Resource Engineering, Inc.[1]
Intelligent Security Systems, Inc.[1]
Iomega Corporation[1]
MOBIUS Encryption Technologies[1]
Personal Computer Card Corporation[1]
Secure-It, Inc.[1]
Security Dynamics Technologies, Inc.[1]
SmartDisk[1]
Technical Communications, Inc.[1]
Wang Federal, Inc.[1]

B
FAX Security

Blue Star Marketing, Inc.[1]

Digital Equipment Corporation[2]

© 1995 by INPUT. Reproduction Prohibited.

Karcher Group, Inc.'

Ricoh Corporation'

Vocal Telecommunications'

Wang Federal, Inc.'

C
Secure LANS

Digital Equipment Corporation'

EDS'

GRI Secure Communications'

IMC Networks Corporation'

Tektronix, Inc.'

Thomas Engineering Company'

Wang Federal, Inc.'

D
Secure Modems

Blue Star Marketing, Inc.'

General DataComm Services, Inc.'

Versitron'

Wang Federal, Inc.'

DATA:

Blue Star Marketing, Inc.'

Digital Equipment Corporation'

General DataComm Syatems, Inc.'

Wang Federal, Inc.'

© 1995 by INPUT. Reproduction Prohibited.

FAX:

Blue Star Marketing, Inc.'

Digital Equipment Corporation'

General DataComm Systems, Inc.'

Wang Federal, Inc.'

E
Security Software

Application Configured Computer, Inc.'

Axent Technologies'

Baker Audio/Telecom'

Banyan Systems, Inc.'

Centel Federal Systems, Inc.'

Cheyenne Software, Inc.'

Command Software Systems, Inc.'

Computer Associates International'

Data General Corporation'

Expert Systems Software, Inc.'

Fischer International Systems Corp.'

Information Resource Engineering, Inc.'

Informix Federal'

Intelligent Security Systems, Inc.'

International Business Machines1'

Lassen Software, Inc.'

Memory Products and More'

Mergent International, Inc.'

© 1995 by INPUT. Reproduction Prohibited.

MOBIUS Encryption Technologies[1]

Novell, Inc.[1]

Oracle Corporation[1]

Personal Computer Card Corporation[1]

Safetynet, Inc.[1]

Secure-It, Inc.[1]

Security Dynamics Technologies, Inc.[1]

Software AG Federal Systems, Inc.[1]

SUN Microsystems Federal, Inc.[1]

Symantec Corporation[1]

Tektronix, Inc.[3]

usrEZ[1]

Wang Federal, Inc.[1]

F
Security Systems Software

Argus Systems Group, Inc.[1]

Blue Lance, Inc.[1]

Centel Federal Systems, Inc.[1]

Computer Information Systems, Inc. (CIS, Inc.)[1]

Command Software Systems, Inc.[1,4]

CompuAdd Corporation[1]

Computer Associates International[1]

CSS Laboratories, Inc.[1]

Data General Corporation[1]

Digital Equipment Corporation[1]

© 1995 by INPUT. Reproduction Prohibited.

Hewlett Packard Company[5]

Information Resource Engineering, Inc.[1]

Intelligent Security Systems, Inc.[1]

International Business Machines (IBM)[1]

Novell, Inc.[1]

Personal Computer Card Corp.[1]

Rimage Corporation[1]

Safetynet, Inc.[1]

The Santa Cruz Operation, Inc. (SCO)[1]

Secure-It, Inc.[1]

Security Dynamics Technologies, Inc.[1]

SUN Microsystems Federal, Inc.[1]

Tektronix, Inc.[3]

Wang Federal, Inc.[1]

G
Security Consulting

Computer Associates International[7]

Harris Computer Services Division[7]

1 *GSA Schedule Contract*
2 *CHCS (Composite Health Care System), SAIC/DoD*
3 *SEWP (Scientific & Engineering Workstation), Harris Computer Systems/ NASA*
4 *Companion (Standard Desktop Computer Contract), GTSI/Navy*
5 *Super Minicomputer Program, PRC/Navy*
6 *ULANA II, EDS/Air Force*
7 *TAC-4 (Tactical Advanced Computer 4), Hewlett-Packard/Navy*

Source: Government Computer News, FY 96 Contracts Sourcing Guide

© 1995 by INPUT. Reproduction Prohibited.

(Blank)

© 1995 by INPUT. Reproduction Prohibited.

INPUT®

Clients make informed decisions more quickly and economically by using INPUT's services. Since 1974, information technology (IT) users and vendors throughout the world have relied on INPUT for data, research, objective analysis and insightful opinions to prepare their plans, market assessments and business directions, particularly in computer software and services.

Contact us today to learn how your company can use INPUT's knowledge and experience to grow and profit in the revolutionary IT world of the 1990s.

Subscription Services

- Information Services Markets
  - Worldwide and country data
  - Vertical industry analysis
- Systems Integration/Professional Services Markets
- Client/Server Software
- Outsourcing Markets
- Information Services Vendor Profiles and Analysis
- Electronic Commerce/Internet
- U.S. Federal Government IT Markets
- IT Customer Services Directions (Europe)

Service Features

- Research-based reports on trends, etc. (More than 100 in-depth reports per year)
- Frequent bulletins on events, issues, etc.
- 5-year market forecasts
- Competitive analysis
- Access to experienced consultants
- Immediate answers to questions
- On-site presentations

Databases

- Software and Services Market Forecasts
- Software and Services Vendors
- U.S. Federal Government
  - Procurement Plans (PAR, APR)
  - Forecasts
  - Awards (FAIT)

Custom Projects

For Vendors—analyze:

- Market strategies and tactics
- Product/service opportunities
- Customer satisfaction levels
- Competitive positioning
- Acquisition targets

For Buyers—evaluate:

- Specific vendor capabilities
- Outsourcing options
- Systems plans
- Peer position

Other Services

Acquisition/partnership searches

INPUT Worldwide

Frankfurt
Perchstätten 16
D-35428
Langgöns
Germany
Tel. +49 6403-911-420
Fax +49 6403-911-413

London
Cornwall House
55-77 High Street
Slough, Berkshire
SL1 1DZ, England
Tel. +44 (0) 1753 530444
Fax +44 (0) 1753 577311

New York
400 Frank W. Burr Blvd.
Teaneck, NJ 07666
U.S.A.
Tel. 1 (201) 801-0050
Fax 1 (201) 801-0441

Paris
24, avenue du Recteur Poincaré
75016 Paris
France
Tel. +33 (1) 46 47 65 65
Fax +33 (1) 46 47 69 50

San Francisco
1881 Landings Drive
Mountain View
CA 94043-0848
U.S.A.
Tel. 1 (415) 961-3300
Fax 1 (415) 961-3966

Tokyo
Saida Building, 4-6,
Kanda Sakuma-cho
Chiyoda-ku, Tokyo 101
Japan
Tel. +81 3 3864-0531
Fax +81 3 3864-4114

Washington, D.C.
1921 Gallows Road
Suite 250
Vienna, VA 22182-3900
U.S.A.
Tel. 1 (703) 847-6870
Fax 1 (703) 847-6872